Department of Political Science

Department of Philosophy and Social Sciences

International Organization and Human Rights

A blurring line between biological and cyber threats: a legal analysis of the international cyber-biodefence strategy

Supervisors

Prof. Pietro Pustorino

Prof. Joe Burton

Co-supervisor

Prof.ssa. Elena Sciso

Arianna Mandile

LUISS Student ID 645132

ULB Student ID 000539113

Academic Year 2021/2022

Index

Introduction

Over the past two decades, there has been much discussion about the implications of technological advances across a variety of fields, including biotechnology, Artificial Intelligence (AI) and Information and Communications Technology (ICT), to name a few. Mainly centered on collecting, processing and storing enormous amounts of data, these innovations have promised multiple economic and social benefits, improved efficiency and accelerated productivity while mounting concerns about their dual-use potential. The increased connectivity and convergence of cyber and biological sciences have indeed lowered access barriers to technological capabilities, broadening the risks of exploitation and disruption.

Of major concern is the greater exposure of digitized biological data to cyberattacks and technical breakdowns, opening tremendous avenues for a new generation of biological weapons. Researchers have already demonstrated bioweapon capabilities in: (*i*) creating ex novo pathogenic viruses, (*ii*) manipulating bacteria engineering to make them more dangerous, and (*iii*) producing microbes to release toxin materials, all with devastating ecological and societal impacts. This trend has fueled hybrid challenges and security issues, affecting the character of warfare combining elements of unexpectedness and asymmetry.

Meanwhile, the rate of technological innovation and the explosion of big data have outstripped the ability of the existing multilateral system to monitor and evaluate pervasive cyber and bio risks. Continuous advances in technology might simultaneously increase the sophistication and accessibility of malicious attacks, disturbing the values upon which regulatory and legal frameworks are based on. Some technological domains are already governed by complex defence frameworks, political agreements, research principles and technical, ecological and human rights standards, but rarely provide adequate responses to emerging hybrid treats. Significant aspects of this regime continue to be challenged, arising grey areas deliberately exploited to minimize legal, military and political consequences.

The present thesis aims at analysing the current international cyber-biodefence legal regime and testing its effectiveness over the emerging trend of technological convergence. After a brief historical excursus on the fourth industrial revolution's technologies, the first chapter explores the increasing dependency of biological sciences on computer networks and the spawning of a new hybridized discipline investigating and mitigating emerging security vulnerabilities.

Besides bio hybrid threats, the pervasive development of converging technologies has raised multiple legal questions and concerns. The second chapter investigates the international legal framework governing cyber warfare and cyberspace, highlighting normative gaps and major shortcomings in

ensuring compliance regulations, while the third section deals with the international bio defence regime and the increasing challenges of dual use research and technology. Finally, the last section focuses on emerging hybrid threats and the potential implications on human rights and fundamental freedoms, concluding with some suggestions towards a new strategy.

Chapter 1

A new era of hybrid risks: a growing interdependency between biology and cyberspace

1.1.Technologies of the fourth industrial revolution: a mixture of hope and doubt

The term *revolution* – coming from the Latin world *revolvere* – is generally used to refer to radical and systemic changes arising beyond the political sphere[1]. Human history has been characterized by significant paradigm transitions which have triggered rapid changes in social structures and economic systems[2].

The first profound transition occurred around 10,000 years ago when humans stopped foraging and started farming, paving the way for modern civilization. The shift to agricultural societies was mainly due to the increasing domestication of plants and animals, replacing hunting and gathering as the only sources of food procurement. The rise in productivity and agricultural knowledge resulted in unprecedented population growth, contributing to the rise of human settlements and cities[3].

On the back of the agricultural revolution, a succession of industrial revolutions has altered the nature of work across all industries and transformed how people interact with one another and the natural world at large[4].

By the mid-18th century, a real game-changing period started with the emergence of water and steam-powered engines which have radically transformed artisan systems from hand production methods to machine manufacturing. Mostly confined to Britain, this transition is often referred to as the First Industrial Revolution whose increase in capacity and productivity led to the growth of regional and global market economies[5].

Later in the 1800s, the employment of electrically-powered mass production technologies marked the dawn of the Second Revolution, sparking further industrial changes around the world. Besides a boost in manufacturing output, a new wave of system changes proved the transformational potential of

[1] Lawson G., 'Negotiated revolutions: the prospects for radical change in contemporary world politics', (Review of international studies, 2005), 31(3), pp. 476.
[2] Stearns P., *The Industrial Revolution in World History*, (Routledge, 2020), pp. 9-11.
[3] Weisdorf J., 'From Foraging to Farming: Explaining the Neolithic Revolution', (*Journal of Economic Surveys*, 2005), 19(4), pp. 561-563.
[4] Schwab K., *The Fourth Industrial Revolution*, (World Economic Forum, 2016), pp.14-15.
[5] Haradhan M., 'The First Industrial Revolution: Creation of a New Global Human Era', (*Journal of Social Sciences and Humanities*, 2019), 5(4), pp. 377-387.

electricity, which allowed factories to improve transportation and communication technologies and adopt modern production lines[6].

Following the Second World War, revolutionary breakthroughs in digital computing and information theory started the Third Industrial Revolution, opening the door to progressive automation of manufacturing processes. The application of newly sophisticated electronic devices has resulted in greater accuracy and increased speed, enabling an entire production process to be automated without recurring human assistance. Rapid advancements in internet technology have converged with new energy system models, laying the foundational infrastructures for a new interconnected economic paradigm[7].

Building upon the digital capabilities of the third wave, the Fourth Industrial Revolution (hereinafter, 4IR) has recently started, creating a world "*in which virtual and physical systems of manufacturing cooperate with each other in a flexible way at the global level*"[8]. The networking of all systems has resulted in the so-called *cyber-physical production systems*[9] (CPPS) where the continuous development and improvement in information systems have enabled the emergence of interconnected new technological operations. These new intelligent devices can communicate via digital networks using worldwide available services and data, expanding the global network connection[10].

Unique in its scale and complexity, the fourth wave - described by German's *Industry 4.0*[11] – conceptualizes a confluence of physical assets and advanced digital technologies, such as Artificial Intelligence (AI), robotics, the Internet of Things (IoT), 3D printing, genetic engineering and quantum computing that all encourage better optimization of systems. Ultimately, the blurring of lines between the physical, digital, and biological realms has produced realities that we previously considered unthinkable[12]. Impacting virtually every facet of modern life, the 4IR disruptive technologies have become less costly and more accessible, combining technological and human capacities in an unprecedented and powerful way.

---

[6] Swann T., 'Information, cybernetics and the second industrial revolution', (*Ephemera: theory & politics in organization*, 2017), 17(2), pp 457-465.
[7] Haradhan M., 'Third Industrial Revolution Brings Global Development', (*Journal of Social Sciences and Humanities*, 2021), 7(4), pp. 241-242.
[8] Schwab K., *The Fourth Industrial Revolution*, (World Economic Forum, 2016), pp.12.
[9] The term was coined by Helen Gill at the National Science Foundation (NSF) around the early 2000s and it has since been used in academia and industry.
[10] Qin W., Chen S., Peng M., 'Recent advances in Industrial Internet: insights and challenges', (*Digital Communications and Networks*, 2020), 6(1), pp. 1-4.
[11] The term was originally introduced by the German government at the Hannover Fair event, symbolizing the dawn of a new industrial era.
[12] Hinton, S., 'How the Fourth Industrial Revolution is impacting the Future of Work', (*Forbes*, 2018), Available at: < https://www.forbes.com/sites/theyec/2018/10/19/how-the-fourth-industrial-revolution-is-impacting-the-future-of-work/>, (accessed 10 May 2022).

One of the most innovative aspects of the fourth wave is *the internet of Things* (IoT), that is in the words of Schwab "*one of the main bridges between the physical and digital applications enables by the fourth industrial revolution*"[13]. The term denotes an invisible network of physical devices – or things - built-in sensors with the ability to connect and exchange independently data and sensitive information over the Internet[14].

The analogy 'data is the new oil', originally proposed by the British mathematician, Clive Humby in 2006, highlights the role of data as a profitable trade resource that fuels innovation and technology. Today, estimates show billions of IoT devices collecting varied types of personal and health data[15], definitively transforming the way production systems are built, while creating legal challenges and questions around privacy, protection, liability and regulatory issues. As intangible assets, data are not covered by any intellectual property laws, conferring them any ownership right. Data are generally protected to the extent they are a company or trade secret, contain personal or customized data, or are part of a database. Although some authors have amounted data to tangible goods[16], it is unlikely that lawmakers and judges will follow the same trend. Establishing ownership-like protection of data might indeed, protect investments in the digital sector, while seriously affecting the free use and exchange of data[17]. It follows the urgent need to find an appropriate balance between what is legally permissible and societally acceptable.

The core technology behind recent progress is the Artificial Intelligence (AI) industry. The AI term describes the ability of a digital computer to imitate human capabilities, generally borrowing human intelligence characteristics and implementing them as algorithms[18]. It finds application in numerous areas of industry, science and society, working in conjunction with robotics, autonomous vehicles, IoT and other advanced fields. Although the huge upside in the potential of AI, implementation does not come without certain risks to national security and citizens' rights[19]. The very few regulations

[13] Schwab K., *The Fourth Industrial Revolution*, (World Economic Forum, 2016), pp.9.
[14] Vamsidhar E., Karthikeyan C., Banerjee D., 'Introduction to the Internet of things', in Prakash K., *Internet of things: from the foundations to the latest frontiers in research*, (De Gruyter, 2021), pp. 1-4.
[15] Steward J., 'The Ultimate List Of Internet Of Things Statistics For 2022' (*Findstack*, 2022), Available at: <https://findstack.com/internet-of-things statistics/#:~:text=Internet%20of%20Things%20(IoT)%20emerged,and%2075.44%20billion%20by%202025.>,(accessed 13 May 2022).
[16] Xiong F., and others, 'Recognition and Evaluation of Data as Intangible Assets', (*Sage*, 2022), pp. 6-7; McCormack T., 'International Humanitarian Law and the Targeting of Data', (*International Law Studies*, 2018), 94, pp. 237-239.
[17] Al-Khouri A., 'Data Ownership: Who Owns 'My Data'? ', (*International Journal of Management & Information Technology*, 2017), 2(1), pp. 2-5.
[18] Dignum V., *Artificial Intelligence: Foundations, Theory, and Algorithms: how to Develop and Use AI in a Responsible Way*, (Springer, 2019), pp. 9-10.
[19] They mainly include justice, equality, integrity, human dignity, freedoms, non-discrimination, privacy, human autonomy and self-determination of the individual.

governing AI, along with the lack of clarification on existing obligations regarding specific uses of AI might soon multiply the adverse impacts[20].

Among essential technologies driving Industry 4.0, there are autonomous transport devices (AVs), ranging from trucks, drones, planes and boats whose high-tech sensors allow them to sense the environment around and navigate without human intervention.

3D printing, also known as Additive Manufacturing (AM), involves producing a three-dimensional solid object from a digital model by laying down layer upon layer until the final object is built. Over the last two decades, innovative AM techniques have been employed in the automotive, aerospace, energy marine, and medical sectors, resulting in increasing industry applications. Extensive research is already working on 4D printing technology, which will allow a multi-material object to transform its form or function over the influence of external stimuli.

Advanced robotics are deployed in various industries, including aerospace, nursing, food, civil engineering, and agriculture. By entering a sequence of instructions, robots are capable of performing automatically a variety of tasks and movements, demanding intense human-robot cooperation in industrial environments.

The aforementioned developments of additional equipment have increased the potential of the robotics industry, whose success has stimulated research of new non-manufacturing applications in various areas[21]. Helping to improve the levels of efficiency and productivity, the total number of robots operating in factories worldwide hit a record of 2.7 million in 2020[22].

Furthermore, another sector that shouldn't be ignored is the nanotechnology industry. The term implies the creation and manipulation of the physical and chemicals properties of molecules - a particle or a nanoparticle. It offers sizeable applications in the field of energy, medicine, agriculture, food processing, manufacturing, cosmetics, textiles, construction and aerospace, making significant contributions to human lives[23]. Its progressive convergence with the biotechnology sector – which includes molecular biology[24], gene editing[25], genetic[26] and synthetic biology – stimulates innovative

[20] Rodrigues R., 'Legal and human rights issues of AI: Gaps, challenges and vulnerabilities', (*Journal of Responsible Technology*, 2020), 4, pp. 2-5.
[21] Javaid M., Haleem A., Singh R., Suman R., 'Substantial capabilities of robotics in enhancing industry 4.0 implementation', (*Cognitive Robotics*, 2021), 1, pp. 58-75.
[22] Dzedzickis A. and others, 'Advanced Applications of Industrial Robotics: New Trends and Possibilities', (Applied Sciences, 2021), 12(1), pp.1.
[23] Singh P. and Jairath G., and Ahlawat S., 'Nanotechnology: a future tool to improve quality and safety in meat industry', (*Journal of Food Science and Technology*, 2016), 53(4), pp. 1739–1749.
[24] It is a branch of biology that studies the chemical structures, functions and interactions of living things at a molecular level.
[25] Also called genome editing, it's a new research area seeking to manipulate DNA sequences in the genome of a living organism.
[26] It deals with the study of genes and heredity.

solutions. Without any doubt, the latter represents one of the most explored biotechnology fields as it creates devices or organisms mimicking the natural biological systems.

Technological advancements have driven a new phase of globalization - G*lobalization 4.0*[27] - shaping new risks and opportunities[28]. While the high degree of technological interconnectedness has shrunk distances, opening up borders, it has equally exposed network societies to both traditional and new vulnerabilities.

Major changes are visible in the business environment as well as in people's daily lives. Production processes got faster, cheaper and more efficient, which has resulted in better profitability. Agility and innovation powered by increasing computing performance and management of data have assured higher quality products and rapid reaction to market changes. Hence, the benefits of wireless connectivity have fostered competitiveness worldwide, boosting significant economic and social opportunities[29].

The drop in transportation and communication costs has facilitated the access of small and medium-sized enterprises to new supply chains, expanding existing and new markets with a higher variety and quantity of products and services. Digital platforms have increased labour demand by providing new and well-paid jobs in innovative technology industries, reducing the fear of job loss due to automation and contributing significantly to the global fight against poverty[30].

Significant progress has been made in the health sector, improving the service quality and life expectancy. New innovative techniques, which include biometric technology and genetic engineering among others, have changed the methods of diagnosis and treatment, reducing the number of patients in need of hospitalization and thus the overall costs of medical services[31].

Digital technology has also made education more accessible for millions of students in both developing and developed countries, allowing them to improve their knowledge and skills by participating in distant learning and training programs. As a result, barriers to accessing a high-quality education have universally decreased, positively impacting the fight against inequities and discrimination between countries and socioeconomic classes[32].

Overall, lifestyle quality increasingly improved, registering a sustained rise in real income per person.

---

[27] The term was originally employed for the World Economic Forum Annual Meeting in Davos in 2019.

[28] Kumari S., Goel H., 'Exploring the Architecture of Fourth Industrial Revolution: Globalization 4.0', (*Journal of International Business*, 2020), 7(2), pp. 161-173.

[29] Bertschek I., and others, 'The Economic Impacts of Telecommunications Networks and Broadband Internet', (*Center for European Economic Research*, 2016), pp. 4-12.

[30] Górka K., Their A. and Łuszczyk M., 'Consequences of the Fourth Industrial Revolution in Social and Economic Development in the 21st Century', in Nogalski B. and Buła P., *Industry 4.0 and Digitalization*, (Jagiellonian University Press, 2021), pp.60-71.

[31] Thimbleby H., 'Technology and the Future of Healthcare', (*Journal of Public Health Research*, 2013), 2(3), pp. 5-8.

[32] Elayyan S. 'The future of education according to the fourth industrial revolution', (Journal of Educational Technology & Online Learning, 2021, pp. 4(1), 23-30.

Despite the many benefits, this new era of increasing interconnectedness and technological advancements has exposed humans to new threats.

Although inequality between countries has significantly diminished since the 1970s, the concentration of wealth within countries varies considerably[33]. It is undeniable that globalization processes have pushed toward the integration of trade, financial markets and consumption patterns, transforming the world into a single market.

Yet, some adverse consequences include the disappearance of small businesses across many factors of the economy, losing the race with foreign competitors. As a consequence, humans are increasingly faced with serious threats in terms of job losses and unemployment rate, whose forecasts are exacerbated by the expanding automation of numerous jobs. Such unstable circumstances might in the long run weaken the rule of law and lead to the explosion of new forms of violence. Indeed, as demonstrated by criminological research, some forms of organized crime can nearly quadruple during economic downturns[34].

What makes this scenario even worse is the changing nature of conflicts that are becoming digital and globally connected. Indeed, the new millennium battles have become *hybrid* in nature[35], combining traditional battlefield techniques with informational and cyber warfare elements[36].

As the digital world becomes more sophisticated and intertwined, societies are presented with growing cyber threats that are outpacing their ability to mitigate the attendant risks. As a result, the rapid growth of cyber-physical systems and their integration into critical infrastructures have opened up gateways to hackers and malicious actors[37], questioning the rule of law and existing crisis-management mechanisms. Despite increasing concerns about online activity risks, States haven't reached an agreement on a common framework dealing with cybercrime, further fostering tensions and divergencies. Although a number of initiatives have been implemented, they have ignored the structural legal issues causing insecurity[38].

---

[33] Goda T., 'The global concentration of wealth', (*Cambridge Journal of Economics*, 2018), 42(1), pp. 98-100.

[34] United Nations Office on Drugs and Crime, Malby S. and Davis P., 'Monitoring the Impact of Economic Crisis on Crime', (2012), pp. 16-19.

[35] The Gulf War in the 90s marked the changing nature of the conflict, introducing semi-autonomous weapons systems and artificial intelligence on the battlefield.
O' Birkeland J., 'The Concept of Autonomy and the Changing Character of War', (*Oslo Law Review*, 2018), 5(2), pp. 73-88.

[36] Hoffman F., 'Conflict in the 21st Century: The Rise of Hybrid Wars', (*Potomac Institute for Policy Studies*, 2007), pp. 17-25.

[37] Djenna A., Harous S., and Eddine Saidouni D., 'Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure', (*Appl. Sci*. 2021), 11(4580), pp.1-4.

[38]Kavanagh C., 'New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses? ', (*Carnegie*, 2019), pp. 23-24.

Major threats to individual and societal security come from the 4.0 technologies, whose development has enhanced the potential for a new generation of nano and bioweapons. Likewise, diseases have gone global as the abolition of borders makes it harder to track and control infectious diseases. The severity of all these dangers is exacerbated by uncontrolled migrant flows produced by Industry 4.0[39], which have a direct impact on the rise in crime rates and other migration-related crimes.

Fourth Industrial Revolution advances are blurring boundaries across industries, bringing new compliance challenges, which, in turn, require law changes. The protection of human rights is certainly one of the core subject matters, but numerous challenging aspects are yet to be uncovered.

1.1.1. Exponential advancements and a growing threat of biological weapons

The use of contagious diseases and biotoxins in warfare goes back to the early 600 BC when the Athenians poisoned the city's water supplies with black Helleborus roots. Some two hundred years later, in the Middle East, the Hittites became known for having produced the first documented biological weapon by sending infected rams to weaken their enemies[40].

Since then, several more attempts of pathogenic bacteria use have been reported in the early and middle modern ages[41], although the poor scientific knowledge made these crude offensive techniques still of limited military effectiveness.

That being said, the greatest advancement in biological warfare capabilities occurred in the early 1900s when Louis Pasteur and Robert Koch's discoveries in microbiology demonstrated the *Germ Theory* of diseases that finally established a causal relationship between specific microorganisms – known as germs or pathogens - and some diseases, finally providing the scientific foundations for the employment of biological agents as weapons[42].

Commonly referred to as *germ weapons,* - namely "*microorganisms that are produced and released deliberately to cause disease and death in humans, animals or plants*"[43]- biological warfare agents

[39] Migrant populations from poor countries with a high disease burden are considered the key causal factor in the global spread of diseases. As the global population keeps growing, along with social disparities between poor and rich countries, growing migration flows will move in search of a better quality of life, thus affecting the transmission and spread of infectious diseases. Meanwhile, modern transportation modes will increase the speed of people moving, impacting on the incidence rates of infectious diseases.
Knobler S. and others, *The Impact of Globalization on Infectious Disease Emergence and Control: Exploring the Consequences and Opportunities*, (The national Academic Press, 2006), pp. 20-23.

[40] Barras V., Greub G., 'History of biological warfare and bioterrorism', (*Clinical Microbiology and Infection*, 2014), 20(6), pp. 497-502.

[41] In 1347, Mongol forces throwed infested corpses into the Black Sea port of Caffa, with the hope to kill everyone inside. Similarly, in 1710 a Russian army hurled infected bodies over the Swedish troops, and some years later, during Pontiac's uprising (1763), British troops used infected blankets against the Indians, causing an epidemic.

[42] Snowden F., 'The Germ Theory of Disease' in *Epidemics and Society: From the Black Death to the Present*, (Yale University Press, 2019), pp. 204-232.

[43] Galates I., 'The Misuse and Malicious Uses of the New Biotechnologies', (*Cairn*, 2017), pp. 103.

are a subgroup of a larger class of weapons of mass destruction, which also includes chemical, biological, radiological and nuclear weapons (also known as "CBRN" weapons).

The first decades of the 20th century witnessed the development of biological weapons laboratories for potential military use. Since the end of the Second World War, only six countries[44] have publicly declared the development of sophisticated research and testing programs, although evidence suggests there were a dozen or more. The Germans were the first to embark on a documented Biological Weapon (BW) program at the outbreak of World War I, followed by France, Hungary, Italy, Japan, Poland and certainly the Soviet Union[45]. The Japanese program was definitely the largest, involving many thousands of technicians and experts, both military and civilians[46].

However, increasing concerns over epidemiological risks and their uncontrollable nature gradually prompted States to renounce the possession and use of lethal biological weapons, whose research was mostly confined to defensive measures.

In this regard, the threat of adversaries developing bioweapons encouraged the United Kingdom and a few other Western countries[47] to propose a global prohibition regime. These efforts only gained steam when President Nixon publicly ended America's offensive weapons program in 1969, paving the way to what is today known as the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction[48] (hereinafter, "BWC") finally prohibiting "*the development, production, storage or acquisition of microbial or biological agents and toxins in amounts not justified for prophylactic, protective or other peaceful purposes, as well as the production or use of weapons containing these agents*"[49]. Ratified by 141 nations, it is acknowledged as the first legal instrument controlling the proliferation of biological weapons.

Although the BWC represents a great step forward in preventing biological warfare, it faces numerous challenges in its implementation. One of the major deficiencies is the lack of any formal mechanisms for monitoring treaty compliance which has clearly reduced its ability to unravel the proliferation of BW capabilities[50].

---

[44] Including the United Kingdom, United States, Soviet Union, France, Canada, and Japan.
[45] Carus W., 'A Short History of Biological Warfare: From Pre-History to the 21st Century', (*Center for the Study of Weapons of Mass Destruction*, 2017), pp. 12-13.
[46] King W., and Guillemin J., 'The price of alliance: Anglo-American intelligence cooperation and Imperial Japan's criminal biological warfare programme, 1944–1947', (*Intelligence and National Security*, 2018), 34(2), pp. 263-264.
[47] Including France, Germany and the United States.
[48] United Nations, 'Convention of the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction', New York, (1971), 1015 UNTS, entry into force 26 March 1975
[49] Ibidem, Art. 1.
[50] Meier O., 'Verification of the biological weapons convention: What is needed? ', (Medicine, Conflict and Survival, 2002), 18(2), pp. 178-179.

This deficiency results in limited publicly available data on illegal BW activities that can be easily hidden and disguised, making it harder for intelligence agencies to uncover their existence and determine whether they are offensive or defensive programs[51]. As a matter of fact, Western intelligence services misidentified the Soviet Union's large biological weapons program and smaller programs in Iraq, Rhodesia, Chile and South Africa[52].

Despite the uncertainties in listing suspected BW proliferators, today's intelligence activities claim numerous countries in the highly volatile Middle East, as well as in China, Russia, and North Korea, pursuing offensive programs or developing BW capability[53]. No wonder the reason behind BW research projects is mainly driven by geopolitical rivalry rather than a desire to meet public health needs.

Enormous investments in scientific research projects resulted in exponentially growing advancements in biology and biotechnology which has become today a worldwide multibillion-dollar industry[54].

Nonetheless, the convergence of information technology with biological sciences has revealed the dual-use potentiality of biological weaponry. Indeed, although the promises to revolutionise the world and eradicate deadly diseases, life sciences discoveries have unleashed new threats in the form of artificially designed pathogens whose communicability, transmissibility and resistance provide them with a strategic advantage[55].

Specifically, what concerns governments and scientists the most are the multiple techniques of molecular genetics, gene-splicing therapy and genome sequencing which enable the synthesis and manipulation of infectious diseases, allowing for *super bugs* with increased virulence and resistance to vaccines or antibiotics[56].

Put simply, genetic engineering "*is the process of human intervention to transfer functional genes (DNA) between two biological organisms (…) allowing for the manipulation of genes to create new pathogenic characteristics*"[57].

Furthermore, the growing interest in biological sciences has given birth to biotechnological social movements – such as the biohackers community, commonly known under the name of "Do-it-

[51] Lentzos F., 'Compliance and Enforcement in the Biological Weapons Regime', (*UNIDIR*, 2019), pp. 13-16.
[52] Buccina J., Dylan G. Weber A., 'Biological Deterrence for The Shadow War', (*Texas National Security Review*, 2021).
[53] Stewart P., 'Proliferation of Weapons of Mass Destruction', in *Weak Links: Fragile States, Global Threats and International Security*, (Oxford University Press, 2011), pp. 110-111.
[54] Ostergard R., Tubin M., and Altman J., 'Stealing from the past: globalization, strategic formation and the use of indigenous intellectual property in the biotechnology industry', (*Third World Quarterly*, 2001), 22(4), pp. 645-646.
[55] Sharma A., and others, 'Next generation agents (synthetic agents): Emerging threats and challenges in detection, protection, and decontamination', in S.J.S Flora and Pachauri V., *Handbook on Biological Warfare Preparedness* (*Elsevier*, 2020), pp. 224.
[56] Ryan J., 'Future Directions for Biosecurity', (*Biosecurity and Bioterrorism*, 2016), pp. 345-363.
[57] Michael J. Ainscough, 'Next Generation Bioweapons', (*USAF Counterproliferation Center*, 2002), pp. 1.

yourself biology" - where biological techniques are studied and practiced with the same methods as in traditional research institutions. Within these emerging communities, information, tools and resources are exchanged freely, building a significant level of expertise without a biosafety regulatory framework[58]. Cases of amateurs being accused of pursuing suspecting activities outside of supervised laboratories have recently increased.

According to the *Economist*, "*biohacking' groups are now experimenting with DNA as software they can manipulate the way hackers did with computers and the Internet*"[59], encouraging the potential misinterpretation and hostile misuse of "*these processes to create killer bugs or provide training for bioterrorists*"[60].

Hence, the "*democratization*" of biology is reshaping the relationship between life sciences and society, questioning which regulatory framework may apply. National laws are generally blurred and outdated and do not specifically address DIY-bio laboratories, raising concerns about consumers', research participants' and environmental safety. At the international level, the Biological Weapons Statue[61] allows for reasonably justified exceptions including peaceful research. However, it is unclear whether DIY research falls into this category, leaving de facto the DIY community free of any legal constraints.

As a result, since the early 90s, there has been increasing concern over the expansion of BW to a broad range of individuals – terrorist groups and lone wolves - culturing and exploiting pathogens for military purposes[62]. As many have already expressed concerns of, the biotechnology revolution is transforming the nature of bioterrorism attacks that are highly likely to become a common modus operandi both among extremists and unaffiliated individuals[63].

Interpol has defined bioterrorism as "*the intentional release of biological agents or toxins for the purpose of harming or killing humans, animals or plants with the intent to intimidate or coerce a government or civilian population to further political or social objectives*"[64]. Hence, a bio-attack can

[58] Landrain T. and others, 'Do-it-yourself biology: Challenges and Promises for an Open Science and Technology Movement' in *Systems and Synthetic Biology*, (Springer, 2013), pp. 23-24.
[59] The Economist, 'Improvised weapons. Hell's Kitchens', (2016), Available at: < https://www.economist.com/science-and-technology/2016/05/21/hells-kitchens >, (accessed 18 May 2022).
[60] Frinking E. and others, 'The Increasing Threat of Biological Weapons: Handle with Sufficient and Proportionate Care', (*The Hague Centre for Strategic Studies*, 2016), pp. 13.
[61] United Nations, 'Convention of the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction', New York, (1971), 1015 UNTS, entry into force 26 March 1975
[62] Ibidem, pp. 9-14.
[63] Christopher F. and Greninger A., 'Biotechnology and Bioterrorism: An unprecedented World', (*Survival*, 2004), 46(2), pp. 143-162; Kosal M., 'Emerging Life Sciences and Possible Threats to International Security', (*Elsevier*, 2020), pp. 599-613.
[64] Interpol, 'Bioterrorism Incident Pre-planning and response guide', (2007), pp. 2.

be designed through engineered biology or weaponized bioagents, potentially resulting in a pandemic[65] or epidemic[66].

The tragedy of 2001, followed by anthrax letters mailed through the U.S. Postal Service[67], has brought the fear of *black biology* closer to reality, along with natural diseases humankind has always been faced with. The attack killed five people, while infecting other seventeen, further creating widespread economic and social disruption. It demonstrated to the public the risks of indiscriminate use of infectious diseases, highlighting concern over the potentiality of sophisticated biotechnology advances[68].

With no surprise, many analysts have ranked engineered biological organisms as "*the most dangerous of all existing weapons technologies, with the potential for producing more extensive and devastating effects on human populations than even fusion nuclear weapons*"[69].

Lower costs, together with broad information distribution, a faster rate of development and a reduced need for expertise have progressively incentivized States and non-state actors to invest in biological research. From a technical perspective, the easy access to all the equipment needed and raw materials make the creation of BW relatively easy, thus escaping international surveillance[70]. Hence, synthetic biology advances could easily be of benefit of terrorist groups, using sensitive data to create dangerous pathogens or modifying them into a more virulent weapon.

In 2019, criminal pro-ISIS groups promoted the use of bioweapons through audiovisual campaigns, providing instructions on how to produce and use them[71].

Hence, the 20th century has witnessed the increasing use of more sophisticated biological weapons by non-state actors, becoming one of the key security issues of today's century.

1.1.2. The Covid-19 pandemic and the reawakening of bioweapon fears

It was in late 2019 that a novel coronavirus causing acute respiratory syndrome, SARS-CoV-2, was detected in Wuhan, China, spreading rapidly within China and across the world. Since the first

[65] It is defined as a worldwide spread of an infectious disease.
[66] An epidemic is a sudden disease outbreak in a community or region in a relatively short time period.
[67] Soon after the terrorist attacks of 9/11, an unknown number of letters laced with anthrax were mailed through the U.S. postal system, exposing postal workers to possible harm. Initially, envelopes were ignored till the first victim was diagnosed with anthrax. Over 30,000 people received antibiotic treatment, numerous mails were quarantined, and postal facilities were all cleaned up, amounting to hundreds of millions of dollars.
[68] Stern J., 'Dreaded Risks and the Control of Biological Weapons', (*International Security*, 2002), 27(3), pp. 99-101.
[69] Dudley J., and Woodford M., 'Bioweapons, Biodiversity, And Ecocide: Potential Effects of Biological Weapons on Biological Diversity', (*BioScience*, 2002), 52(7), pp. 583.
[70] Kosal M., 'Emerging Life Sciences and Possible Threats to International Security', (Orbis, 2020), 64(4), pp. 599-561.
[71] Townsend-Drake A., 'Bioterrorism: Applying the Lens of COVID-19', (*Counter Terrorism Preparedness Network, 2021*), pp. 19-20.

few cases were reported, numerous theories about its origins have since been advanced, contributing to what the World Health Organization declared as *infodemic* – "*an overabundance of data, including false or misleading information in digital and physical environments, that makes it hard for people to find trustworthy sources and reliable guidance.*" [72]

Through genetic sequencing, scientists suggested the epidemic was caused by a zoonotic virus – i.e. a virus originating in animals – rapidly transmitted from an animal vector at a live-animal market in Wuhan. The uncertainties around the precise animal source of the virus have called for an investigation into the origin and pathway through which Coronavirus disease emerged, helping scientists reduce its containment and prevent further outbreaks[73].

Yet, the Chinese government's censorship surrounding research on the origins of the Covid-19 has served conspiracy theories and rumours, spreading rapidly through social media. While some speculate about a potentially engineered virus, some others suspect SARS-CoV-2 was produced in a P4 research laboratory[74] in Wuhan previously found to have safety concerns. The idea of the "Chinese virus"[75] has been perpetuated so far, fuelled by numerous other historical incidents from modern research in China – namely the recent announcement of gene editing of babies in late 2018 and the accidental release of SARS from a Beijing laboratory in 2004.

The similarities between viral pandemics and bioweapons have made conspiracy theories look plausible, further powered by China's false allegation of bioweapon labs[76]. Yet, scientific findings don't reveal any sign of human manipulation of the virus, eliminating any narrative possibility of a laboratory leak or a viral bioweapon[77].

Regardless of the truth behind the virus that has so far claimed more than 6,000,000 lives[78], it has revived the threat posed by the intentional or accidental release of bioagents, exacerbated by weak health security where "*over 80% of countries score in the bottom tier – also called low scores - for indicators related to malicious threats*"[79],

---

[72] WHO, 'Situation Report - 13' (2020), pp. 2, Available at: < https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf>, (accessed 21 May 2022).
[73] Haider N., and other, 'Covid-19 – Zoonosis or Emerging Infectious Disease? ', (*Frontiers in Public Health*, 2020), 8, pp. 3-4.
[74] Level 4 laboratories research on infectious agents or toxins causing fatal diseases in humans.
[75] Bolsen T., Palm R., and Kingsland J., 'Framing the Origins of COVID-19', (*Science Communication*, 2020), 42(5), pp. 564.
[76] Knight D., 'COVID-19 Pandemic Origins: Bioweapons and the History of Laboratory Leaks', (*Southern Medical Journal*, 2021), 114(8), pp. 465-466.
[77] Ling J., 'The Lab Leak Theory Doesn't Hold Up', (*Foreign Policy*, 2021), Available at: <https://foreignpolicy.com/2021/06/15/lab-leak-theory-doesnt-hold-up-covid-china/>, (accessed 21 May 2022).
[78] WHO, 'Coronavirus (COVID-19) Dashboard' (*Covid19.who.int*, 2022), Available at: <https://covid19.who.int/>,(accessed 21 May 2022).
[79]Cameron E, Nuzzo J, and Bell J, 'Global Health Security Index' (*Nuclear Threat Initiative, Johns Hopkins Center for Health Security, The Economist Intelligence Unit*, 2019).

Although the WHO has been warning ever since of "*approximately 7,000 signals of potential outbreaks every month*"[80], the coronavirus disease pandemic has exposed serious gaps in global preparedness, unveiling vulnerabilities worldwide.

Biothreats – including bacteria, viruses, pollutants, toxins, plants and others – circulate the globe, potentially triggering adverse effects at any time and anywhere in the world that may not be immediately apparent. Its invisible nature adds complexity, making its detection even harder.

Taking the case of the Ebola epidemic, the latter was only declared a security threat once it had already spread out in urban areas and crossed frontiers[81].

It is worth noting that economic, environmental, and physical factors increase the susceptibility of some regions to biothreats. For instance, climate changes or specific mutations in an infectious agent may play a role in the spread of an outbreak.

Nowadays, population growth, wildlife and microbiological variety all favor the spread of novel infections spontaneously[82].

All these elements, along with advances in technology and biosciences, have reawakened the potential of biological warfare as a terrorist methodology, raising bioterrorism as a widespread concern.

As reported by the United Nations, the SARS-CoV-2 virus, and more generally biological agents, has caught the attention of terrorist cells who integrated Covid-19 into their propaganda, contributing to the spread of misinformation through social media and the dark web, both of which exceed borders. Criminal groups affiliated with Daesh and Al Qaeda have disseminated conspiracy theories claiming that the virus has been sent as a soldier of Allah to punish Islam's enemies[83]. These fears are bolstered by claims of extremist groups urging their members to spread the virus by coughing on targeted individuals.

The difficulty of detecting and tracing biological agents makes them extremely appealing to criminal groups. Although prohibited under international law[84], a bioagent can be surreptitiously disseminated over a large geographical area while causing significant disruption. This allows perpetrators to remain anonymous and escape accountability, which can increase dread and uncertainty in the early stages of an incident when responses begin.

[80] 'The Global Risks Report 2019', (World Economic Forum 2019), Available at: <https://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf>, (accessed 24 May 2022).
[81] International Crisis Group, 'The Politics Behind the Ebola Crisis', Africa Report n° 232, (2015), pp. 19-22.
[82] Townsend-Drake A., 'Bioterrorism: Applying the Lens of COVID-19', (*Counter Terrorism Preparedness Network, 2021*), pp. 12.
[83] United Nations Security Council Counter-Terrorism Committee Executive Directorate, 'The Impact of the COVID-19 Pandemic on Terrorism, Counter-Terrorism and Countering Violent Extremism', (2020), pp. 13-14.
[84] This prohibition is based on the Geneva Gas Protocol (1925) and the Biological Weapons Convention (1972).

Given the above, the failure of governments' response to COVID-19 has encouraged terrorists to fill the void. It follows that "*one of the major fallouts from COVID-19 is the loss of millions of jobs, which fuels uncertainty and anger that far-right extremists may exploit for recruitment*"[85].

Besides accelerating the threat of bioterrorism, the spread of Covid-19 across the globe has been accompanied by increasing numbers of scams and ransomware attacks raising by 151%[86] in 2021, posing serious threats to the global economy and safety. What is interestingly new is how informational attacks have resulted in major biosecurity consequences.

Numerous governments and public health authorities have deployed contract tracing and self-reporting apps employing GPS and location services to monitor and identify persons who have been infected[87]. Although these mechanisms have been expressly designed to contain the spread of the virus, they have raised serious privacy concerns.

China has been the first country to introduce tracking mechanisms to record people's movements. Based on self-reported information, users are sent health QR codes on their phones that indicate their COVID-19 risk level, determining whether or not they have access to public transportation or public locations. Similarly, South Korean residents have been sent flurries of alerts about infected people living nearby, containing detailed information about their age, gender and recent travel destinations[88].

Likewise, disease surveillance data – including medical records, diagnostic test results, and general trend information among other things – has become critical for both policymakers and scientists as they are increasingly targeted by malicious actors who want to either "*suppress or artificially inflate data*"[89].

As underscored during the Covid-19 pandemic, a rapid response can mitigate forthcoming disruptions. If diagnostic test results and surveillance data are altered to keep numbers below alert thresholds, outbreak control mechanisms won't be activated until the infection has grown significantly. Alternatively, the fallacious production of illness cases may mislead the appearance of an outbreak, mobilizing considerable resources to investigate and mitigate the effects needlessly.

It goes without saying that failure to correctly identify potential outbreaks may have catastrophic results. For instance, trade restrictions are usually implemented to block the spread of disease across borders and the erroneous reporting of an outbreak may cause significant trade losses.

---

[85] Cruickshank P., and Rassler D., 'A Virtual Roundtable on COVID-19 and Counterterrorism' (CTL Sentinel, 2020), 13(6), pp. 3-4.

[86] Pomeroy R.., 'Ransomware And 'Ransom-War': Why we must be Ready for Cyberattacks' (*World Economic Forum*, 2022).

[87] Examples include apps *Immuni* in Italy, *StopCovid* in France, *Corona-Warn-App* in Germany, *TraceTogether* in Singapore, *Life fits inside the house* in Turkey, SOS Covid Tool in Ecuador and numerous more.

[88] Youngrim K., Chen Y., 'Liang F., Engineering care in pandemic technogovernance: The politics of care in China and South Korea's COVID-19 tracking apps', (*New Media and Society*, 2017), pp. 3-5.

[89] Trump B. and others, *Emerging Threats of Synthetic Biology and Biotechnology*, (Springer 2021), pp. 109.

All in all, mass digital surveillance practices have raised serious concerns related to the exposure of personal data and the potential breaches of human rights. To increase these fears has been the ineffectiveness of the International Health Regulations[90] (2005), originally designed to strengthen the national capacity to detect and report potential public health emergencies of international concern, while protecting human rights in public health responses. Nevertheless, besides an increasing number of State Parties violating IHR obligations, particularly on preparedness, the World Health Assembly (WHA) has not performed adequately IHR management and supervision activities[91].

This analysis sheds a light on the integrity of the numerous public bioinformatic databases produced so far, where researchers upload and share data for global use. Besides the unintentional insertion of errors into databases, what concerns most is the intentional modification of data which may undermine trust and confidence in the short run[92].

Although the digital revolution has introduced smart laboratories facilitating data sharing, collaboration and connectivity, it has exposed sensitive data to unauthorised access, use and modification, ultimately threatening data integrity and availability[93]. A predictable outcome has been Covid vaccination espionage and intellectual property theft, involving both scientific data and patients' information.

This has resulted in aggressive attacks against the vaccine's supply chain. Forty-four companies – ranging from pharmaceutical firms, biomedical research organizations and medical equipment manufacturers - in fourteen different countries across Asia, North and South America and Europe[94], have been hacked, undermining trust in medical treatments. These facts underscore the weaknesses of cyber and biosecurity practices and policies to face unconventional threats.

Overall, the COVID-19 pandemic has served as a powerful reminder of the potential damage diseases can cause, drawing the attention of the international community on the fact that biohazards can no longer be ignored.

This novel coronavirus's experience reveals that the world community is simply unprepared for the potential consequences of future pandemics, bioweapons, or any other lethal man-made disease.

---

[90] WHO, 'Strengthening preparedness for health emergencies: implementation of the International Health Regulations (2005).

[91] Sohn M., Ro D. and others, 'The problems of International Health Regulations (IHR) in the process of responding to COVID-19 and improvement measures to improve its effectiveness', (*Journal of Global Health Science*, 2021), 3(2).

[92] Pauwel E., 'Cyber-biosecurity: How to protect biotechnology from adversarial AI attacks', (Hybrid CoE, 2021), pp. 4-5.

[93] Kavanagh C., 'New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses? ', (*Carnegie*, 2019), pp. 23-24.

[94] Patterson D., 'Hackers Are Attacking The COVID-19 Vaccine Supply Chain', (*Cbsnews.com*, 2022), Available at: <https://www.cbsnews.com/news/covid-19-vaccine-hackers-supply-chain/ >,(accessed 25 April 2022).

1.2. The convergence of cyber and biological sciences: hybrid threats in the international legal order

Over the last few years, emerging and disruptive technologies (EDTs) along with the evolving nature of digitalization have altered the way conventional and unconventional warfare is conducted, reshaping our understanding of conflict[95].

In recent years, the international security environment has been increasingly facing hybrid threats marked by uncertainty, complexity and ambiguity that have challenged effective response measures. This is, however, not new. As old as warfare itself, hybrid threats have been progressively fuelled by changing security dynamics, new defensive strategies, and emerging technologies[96].

Hence, today's trends of hyperconnectivity and digitalisation have vastly amplified the impact and reach of hybrid tactics that are steadily becoming a desirable strategy for states or non-state actors to pursue their goals.

The unpreparedness of the international order to respond effectively to the challenges hybrid conflicts pose adds a layer of complexity to this fragile framework. All this results in a "*new twilight zone between war and peace*"[97], altering the nature of peace itself.

The terms *hybrid threat* and *hybrid warfare* have been studied through numerous disciplinary perspectives – history and political science, military and security studies to name a few - which blurs the picture of what they really imply.

Overall, the concept of hybrid conflict captures "*a situation in which parties to the conflict refrain from the overt use of armed forces against each other, relying instead on a combination of military intimidation - falling short of an attack - , exploitation of economic and political vulnerabilities, and diplomatic or technological means to pursue their objectives*"[98]. Hence, these tactics allow States to avoid open hostilities whilst still disabling opponents' abilities.

For instance, Russia's intrusive approach to Ukraine marked by diplomatic pressure, economic manipulation and use of insurgencies perfectly illustrates this logic[99].

As hybrid conflict grows worldwide, many States have publicly expressed their intention to deploy hybrid means to actively defend themselves, mirroring how the phenomenon of hybrid warfare is perceived as a threat to the international order.

---

[95] McDevitt M., and others, 'The Changing Nature of Warfare', (*Center for Strategic Studies*, 2004), pp.21-25.
[96] Giannopoulos G., Smith H., and Theocharidou M., 'The Landscape of Hybrid Threats: A Conceptual Model Public Version', (*European Commission*, 2021), pp. 4.
[97] Ibidem, pp.11.
[98] Boehlke T., and Canfor-Dumas E., 'The Military Contribution to The Prevention of Violent Conflict', (*Security and Peace*, 2017), 35(1), pp.7.
[99] Snegovaya M., 'Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare', (*ISW*, 2015), pp. 15-17.

This is translating into the progressive enhancement of national defensive and offensive capabilities worldwide. Russia[100] and China[101] are the states that have most invested in this policy, with a view to widening the scope of hybrid strategies to ensure strategic deterrence, followed by France, Germany the UK, the US, and the Netherlands.

Yet, it is worth noting that such warfare is run in the grey zone of conflict, falling outside the institutional sphere. Indeed, rather than engage public agencies, hybrid operations are generally actualized through non-state players or covert units.

Recently, there has been a notable increase in proxy conflicts[102] where States "*instigate or play a major role in supporting and directing a part to a conflict*"[103], while securing strategic goals without deploying significant extra troops. Hence, proxy wars are labelled as a sub-group of hybrid conflict as states' persistent denial of involvement and the obscuration of the responsibility of groups involved reduces the chances of retaliation. For instance, Russian military intervention in the Syrian civil war has been justified by the need to secure its naval base located in Tartus, together with the patronage networks and clientelism with the Assad regime[104].

Cyberspace has been further invaded by proxy forces, whose attacks have become extremely difficult to attribute, offering states the promise of anonymity.

Hybrid strategies are localized below the threshold of a real confrontation, evading the constructs delineated by international laws. Indeed, traditional legal rules governing interstate armed conflicts so far look out of sync with today's reality. This disparity causes uncertainties in identifying conflict outbreaks, resolving disputes and finding legal remedies.

Following WWII, the new legalist paradigms regulating the *jus ad bellum* – right to wage war - and the *jus in bello* – conduct of parties engaged in an armed conflict - cannot be directly applied and they do not always provide the adequate remedies to hybrid conflicts[105].

---

[100] Trenin D., 'Russia's National Security Strategy: A Manifesto for a New Era', (*Carnegie*, 2021), Available at: <https://carnegiemoscow.org/commentary/84893>, (accessed 26 May 2022).

[101] The State Council Information Office of the People's Republic of China, 'China's National Defense in the New Era' (Xinhua, 2019), Available at: < https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html>, (accessed 15 April 2022).

[102] The term defines a war fought between parties supported and directed indirectly by major powers, influencing the strategic outcome without getting involved in the conflict.

[103] Byman D., 'Why Engage in Proxy War? A State's Perspective', (*Brookings*, 2018), Available at: <https://www.brookings.edu/blog/order-from-chaos/2018/05/21/why-engage-in-roxy-war-a-states-perspective/>,(accessed 26 May 2022).

[104] Frolovskiy D., 'What Putin Really Wants in Syria', (*Foreign Policy*, 2019), Available at: <https://foreignpolicy.com/2019/02/01/what-putin-really-wants-in-syria-russia-assad-strategy-kremlin/>, (accessed 26 May 2022).

[105] Ndi G., 'International Regulation of Armed Conflicts: 'Jus in Bello' in an Age of Increasingly Asymmetric and Hybrid Warfare', (*Journal of Law and Social Sciences*, 2018), 7(1), pp. 3-6.

The important point to bear in mind here is that "*law is an instrument of power and can be utilized as a weapon by law-abiding and non-law-abiding actors alike*"[106]. Thus, states exploit existing legal gaps in the international legal framework to adopt hybrid strategies to pursue their strategic interests, evading – almost - any responsibility.

Four main issues underscore how hybrid activities are insufficiently regulated by international law in its current application.

The first concerns the use of force and State accountability. There is a wide range of cases in which both State and non-state actors – including non-governmental organisations, armed groups and corporations - can be, individually or jointly, held responsible for the violation of legal norms, challenging the determination of responsibility.

That is, the strategic use of proxy actors to influence indirectly conflicts has significant implications as they are not legally and internationally recognized for their accountability.

A non-legally binding framework restating the basic principles of substantive customary and conventional international law concerning State responsibility is provided by the International Law Commission Articles on the Responsibility of States for Internationally Wrongful Acts of 2001 (ILC)[107]. As article 8 of the ILC enshrines "*the conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct*"[108]. The ILC, thus, suggests three disjunctive attribution criteria: (*i*) the issuance of instructions, (*ii*) direction, involving ordering a person and groups to adopt a certain conduct and (*iii*) control over a person or groups. A closer analysis shows the first two standards are extremely specific and easily applicable as they clearly illustrate the type of behaviour required. Differently, the third criterium is ambiguous, resulting in varying interpretations. Of major concern is the lack of a threshold establishing States' overall control over proxy organisations. Overall, the rule is strictly linked to the traditional idea of the State as the only actor with the exclusive right on the legitimate use of force, ignoring actions where no State control is exercised[109].

[106] Torossian B., Fagliano L., and Görder T., 'Hybrid Conflict - Strategic Monitor 2019-2020', (*The Hague Center for Strategic Studies*, 2021).
[107] International Law Commission, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts', (2001), Supplement No. 10 (A/56/10), chp.IV.E.1.
[108] Ibidem, Art.8.
[109] Cassese A., 'The Nicaragua and Tadic Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia', *(The European Journal of International Law*, 2012), 18(4), pp. 664-665.

This trend will progressively normalize proxy conflicts and the ineffectiveness of international law will soon lead to a situation where players rely on alternate means, fuelling instability in the international arena[110].

The second issue covers the non-interference in other States' critical infrastructure, whose number of cases has recently grown. Increasing vulnerabilities in the cybersphere have facilitated the attainment of sensitive data through espionage.

Besides the core principles of international law on state sovereignty, the question of non-intervention is regulated in the Charter of the United Nations, under Art.2(4) and Art.2(7)[111], restricting the power of outside nations to interfere with other nations' affairs. Although elections are not explicitly covered, this principle has gradually included the protection of critical electoral infrastructure as part of a state's sovereignty and stability. Such a principle has been frequently infringed. One of the most remarkable examples being Russia's interference in US presidential elections in 2016, spreading sensitive files and cyber-attacking the Democratic National Committee (DNC)[112].

The third issue deals with the non-discriminatory trade between nations. Despite the prohibition of unfair trade practices, economically coercive measures are being widely employed to achieve national strategic goals, fuelling the range of unlawful hybrid activities evading the constructs set out by international law. The ongoing trade war between China and USA perfectly mirrors this trend.

Legally speaking, the World Trade Organization[113] (WTO) is the only international agency dealing with the global rules of trade. The greatest contribution to the security and predictability of the global economy is given by the dispute settlement system which provides a relatively rapid response to any violation of trade rules, preventing WTO members from acting unilaterally. The recent increase in requests for WTO dispute consultation reflects a clear weakness in the fundamentals of non-discriminatory trade, further jeopardised by economically coercive measures employed worldwide. The overt nature of the trade war the USA and China have been engaged in since 2018 points to an evident paralysis of the dispute settlement body.

Finally, the fourth issue challenging the international legal framework concerns the non-interference in societal affairs of foreign states.

---

[110] Fogt M., 'Legal Challenges or "Gaps" by Countering Hybrid Warfare – Building Resilience in Jus Ante Bellum', (*Southwestern Journal of International Law*, 2020), pp. 60-62.

[111] United Nations, 'Charter of the United Nations', San Francisco, (1945), 1 UNTS XVI, entry into force 14 October 1945, Art.2.

[112] US Senate Select Committee on Intelligence, 'Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations', (2018).

[113] Marrakesh Agreement Establishing the World Trade Organization, Marrakesh (1994), 1867 U.N.T.S. 154, 33 I.L.M. 1144, entry into force 1 January 1995.

Since the Nicaragua v United States case in 1986[114], the International Court of Justice (ICJ)'s findings extended the non-interference principle to economic and civil domains, by affirming "*a prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy*"[115].
It follows that states are forbidden from intervening – whether directly or not – in internal and external matters of other nations.

Nonetheless, states have increasingly relied on disinformation campaigns progressively expanding their reach and frequency, with the purpose of undermining adversaries. Recently, the international community has actively reacted to this emerging trend, further fuelled by cyber advances. In this regards, Rule 10 of the Tallinn Manual 2.0 – dealing with cyber operations both in armed conflicts and peacetime - stipulates that "*a cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations is unlawful*"[116].
Despite international efforts, the reality reflects an overt non-observance of the norm of non-interference.

The recent convergence of cyber and biological science has further expanded vulnerabilities adversaries can easily exploit through grey zone warfare strategies, resulting in consequences that analysts have not yet considered[117].
Activities in the grey zone environment are difficult to detect and attribute, which makes mitigation even more challenging. All these factors combined suggest grey zone tactics are likely to become the most common weapons in the twenty-first century[118].

1.2.1. Defining Cyber-biosecurity: a new emerging hybridized discipline

In the last few years, a confluence of advances in biology and biotechnology has fuelled a new wave of innovation driven by rapid increases in computing power, automation, AI and data analytics.

[114] International Court of Justice (ICJ), 'Case Concerning Military and Paramilitary Activities in and against Nicaragua' (Nicaragua v. United States of America), 27 June 1986.
[115] Ibidem, para. 205.
[116] NATO Cooperative Cyber Defence Centre of Excellence, 'Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0', (2017).
[117] Dixon T., 'The grey zone of cyber-biological security', (*International Affairs*, 2021), 97(3), pp. 687-689.
[118] Belo D., War's Future: The Risks and Rewards of Grey Zone Conflict and Hybrid Warfare, (*Canadian Global Affairs Institute*, 2018), pp. 2-4.

Convergence results when various scientific disciplines interconnect through synergies, promising new capabilities[119].

It is undeniable that the Bio Revolution has helped improve international response to global challenges, opening up a new array of capabilities in the healthcare, agriculture, automation and energy sectors. Recently, bio innovations have been successfully deployed in response to the novel coronavirus in early 2020, which have allowed for a faster understanding of its genesis and transmission patterns, along with more effective therapies.

Yet, the growing interconnectedness between biology and cyberspace has challenged traditional security constructs, multiplying concerns about malicious and unethical activities.

Even prior to the coronavirus pandemic, the US Bipartisan Commission on Biodefense, together with the UK-based Centre for the Study of Existential Risk were investigating the issue. The former held a hearing in 2019 titled *Cyberbio convergence: characterising the multiplicative threat*[120], aiming at providing a greater understanding of the ongoing convergence between information technology (IT) and life sciences, whereas the latter undertook two significant horizon-scanning surveys.[121]

Experts in cybersecurity and biosecurity are not generally familiar with each other's priorities and expertise. Traditionally, cybersecurity encompasses the protection of information technologies, ranging from personal computers and communication devices to public infrastructure and networks. Cyber-physical security addresses the risks threatening the dependency between physical systems and computer-based algorithms that can monitor and manipulate processes. Whereas biosecurity represents a distinct field that focuses on mitigating the risks related to the misuse of science with potential risks to humans, plants, animals and the environment through the intentional or unintentional release of disease agents[122].

Recent investigations have raised concerns over the growing reliance of life sciences on computer-controlled instruments, that is found to expose biological data to cyber vulnerabilities, spawning a new area of cyber-bio risks.

---

[119] Park H., 'Technology convergence, open innovation, and dynamic economy', (*Journal of Open Innovation: Technology, Market, and Complexity*, 2017), 3(24), pp. 7-9.

[120] Bipartisan Commission on Biodefence, 'Cyberbio Convergence: Characterizing the Multiplicative Threat', Washington, (2019); Available at: <https://biodefensecommission.org/events/cyberbio-convergence-characterizing-the-multiplicative-threat/>, (accessed 22 May 2022).

[121] Wintle B. and others, 'A Transatlantic Perspective on 20 Emerging Issues in Biological Engineering' (*eLife*, 2017), 6: Kemp L. and others, 'Bioengineering Horizon Scan 2020', (*eLife*, 2020), 9.

[122] Mueller S., 'Facing the 2020 pandemic: What does cyberbiosecurity want us to know to safeguard the future?' (Biosafety and Health, 2021), 3(1), pp. 11-13.

The notion of *cyber-biosafety* or *bio-cybersecurity* was first used in 2018, with the aim of warning about hybrid risks emerging "at the frontier between cyberspace and biology"[123].

Initially, it has been proposed as a new hybrid discipline that aims to "*understand the vulnerabilities to unwanted surveillance, intrusions, and malicious and harmful activities which can occur within or at the interfaces of comingled life and medical sciences, cyber, cyber-physical, supply chain and infrastructure systems*" and, as such, it helps "*develop and institute measures to prevent, protect against, mitigate, investigate, and attribute such threats as it pertains to security, competitiveness, and resilience*"[124].

More broadly, the term captures interdependencies as risk multipliers, exposing the operating system to a broader risk environment. Hence, cyber-biosecurity aims to identify and mitigate the cyber risks of digitally stored biological information, including genomic, health care and medical data, along with scientific research.

Moving far beyond the cyber and biosecurity domains, it encompasses numerous sectors ranging from energy, artificial intelligence, agriculture, and medicine to environmental health.

Consequently, the notion has been referred to as "*the cyber vulnerabilities associated with networked data systems, laboratory equipment and facility security and engineering controls that may result in environmental contamination or pose a threat to the health of humans, animals. and plants including the health of building occupants, the surrounding community, and/or users and consumers of products created by the life science enterprise*"[125]. The latter version is intended to be inclusive of biosafety and biosecurity principles, blurring the lines between the two terms of safety and security.

While the risks of stealing private and valuable data are well recognized, the biosecurity implications of cyber-attacks appear to be largely elusive to the majority of the agricultural, health and scientific communities. It has only been recently that researchers have developed awareness of severe vulnerabilities accompanying technological advances.

The cyber-physical nature of biological sciences has placed greater attention on data, whose accessibility through various cloud applications lacking adequate cybersecurity increases risks of accidental or deliberate harm[126].

---

[123] Peccoud J., and others, 'Cyberbiosecurity: From Naive Trust to Risk Awareness', (*Trends in Biotechnology*, 2018), 36(1), p.3.

[124] Murch R. and others, 'Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy' (*Frontiers in Bioengineering and Biotechnology*, 2018), 6(39), pp. 3.

[125] Reed J. and Dunaway N., 'Cyberbiosecurity Implications for the Laboratory of The Future', (Frontiers in Bioengineering and Biotechnology, 2017), 7(182), pp. 4.

[126] Carreras N. and others, 'Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis', (*The Journal of the International Council on Systems Engineering*, 2019), 23(2), pp. 189-210.

The potential for exploitation lies exactly where bioengineering processes confluence with both the physical and cyber domains. Unsecured networks and databases might be easily infiltrated by malicious actors, who can remotely manipulate valuable data, resulting in harmful biological outcomes[127].

Numerous countries have been pursuing dual-use research for biological warfare purposes, which has caused cyber incidents severely affecting the private and public sectors. A significant increase has been observed in the number of attacks involving DNA spoofing and camouflaged actions by simulating common disease symptoms.

All in all, the cross-over effects of cyber-bio threats have boosted a new way of thinking that merges physical, biological and cyber elements.

Existing strategies addressing cyber and bio risks represent an important layer, but they don't sufficiently capture the emerging systems and their consequences.

Cyber-bio security is neither a cyber-only nor a biology-only science, but it acts on the edge of these two broad disciplines, sitting outside the international arms control-regime, namely the one governed by the Biological Weapon Convention[128] (BWC), the Chemical Weapons Convention[129] (CWC); furthermore one shall take into consideration also the UN Security Council Resolution 1540[130].

As a result, developing a clear understanding of cyber-biological capabilities is a required step to anticipating future grey zone warfare strategies, whose ambiguous boundaries can be easily exploited by sophisticated actors for uses that are plausibly denied.

Notably, what characterizes a grey zone is its "*ambiguous, political and legal psychological status*"[131], which exploits its undefined and legally equivocal spaces as neither entirely definite nor fully clandestine.

Across the coming decades, the grey zone use of offensive cyber-biological capabilities might demand existing international regulations to adequate rules to the new cyber-bio paradigm.

As formally defined by the US Office of the Secretary of Defence in 2016, the grey zone is "*a conceptual space between peace and war, occurring when actors purposefully use multiple elements of power to achieve political–security objectives with activities that are ambiguous or cloud*

[127] Murch R. and others, 'Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy' (*Frontiers in Bioengineering and Biotechnology*, 2018), 6(39), pp. 4.
[128] United Nations, 'Convention of the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction', New York, (1971), 1015 UNTS, entry into force 26 March 1975.
[129] Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, Geneva, (1992), 1975 UNTS 45, entry into force 29 April 1997.
[130] UN Security Council, 'Security Council resolution 1540', 28 April 2004, S/RES/1540.
[131] Dixon T., 'The grey zone of cyber-biological security', (*International Affairs*, 2021), 97(3), pp. 680-683.

attribution and exceed the threshold of ordinary competition, yet fall below the level of large-scale direct military conflict"[132].

While biological capabilities are largely covered by the BWC, targeting states may find it difficult to "*attribute use in a timely manner without their own technologically advanced defensive cyber-biological capabilities*"[133].

In short, while emerging capabilities in biotechnology have the potential to revolutionize numerous sectors, they also present a tremendous opportunity for dual-use research. States will need to engage closely with their scientific community to ensure that they are appropriately assessing enemy states' technological capabilities and the implications of life sciences research.

Despite the increasing awareness about the potential misuses of scientific research, it appears rather difficult to assess the defensive and offensive uses of cyber-biological data. States are placing attention on the issue, as witnessed by emerging regulations that either secure or exploit genomic data and biological vulnerabilities.

For instance, China defined a new regulatory framework of data protection in 2017[134], and Beijing has also implemented genomic surveillance and collection programs[135]. Likewise, the United States has allowed law enforcement agencies to enter DNA databases of various companies, allowing European descendants to identify familial relatives by using genomic data of millions of individuals. Yet, the state surveillance on medical and healthcare data represents a growing intrusion on personal privacy, unravelling ethical and legal problems.

In summary, as cyber and biological systems evolve, emerging biological vulnerabilities are opening new gaps in the existing arms control regimes which are highly likely to widen over time. This operating environment could easily lead to the development of new offensive capabilities "disrupting disease surveillance systems, compromise medical response systems or attack vaccine manufacturing supply chains"[136].

[132] Ibidem.
[133] Ibidem.
[134] The National People's Congress of the People's Republic of China, 'Data Security Law of the People's Republic of China', (2021), Available at: <http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml>. (accessed 24 May 2022).
[135] Dirks E., and Leibold J., 'Genomic Surveillance: Inside China's DNA Dragnet', (*International Cyber Policy Centre*, 2020), 34, pp. 3-7.
[136] Ibidem.

1.2.2. Assessing vulnerabilities and new cyber-biological risks

The increasing convergence of biological and technological sciences and sophisticated techniques comes with profound risks on entire ecosystems.

Since the H5N1 flu outbreak in 2012, the American security guru, Bruce Schneier, first underscored how cybersecurity practices were progressively applying to the biological domain[137], challenging the traditional understandings of information.

Recently, there has been an upward trend in the number of cyber security incidents, negatively impacting the political, social and economic spheres. Now that biology has become a big data science, largely dependent on computer networks and information technology solutions, it is significantly sensitive to cyber threats.

Unsurprisingly, the healthcare industry has been increasingly targeted by cyber-attacks, ranging from malwares compromising the system integrity they infect to distributed denial of service (DDoS) interrupting the traffic of patient care services.

The COVID-19 pandemic has offered a perfect storm for hackers who exploited network vulnerabilities of companies developing vaccines and experimental therapeutics. Samplings of how AI has facilitated the manipulation of medical databases are malicious attacks on hospitals, resulting in a misdiagnosis rate of more than 90%[138].

Remote work has hastened the adoption of platforms and cloud-based services where to share sensitive data, challenging businesses' security. As broadly acknowledged, cloud computing has revolutionized the using, storing and sharing of data and resources, making them accessible from various locations.

However, this transition has raised various security concerns about malicious attacks on hardware and communication equipment, through which cyber threat actors (CTA) gain unlawful access to users' servers. The initial rush towards a remote workplace environment, combined with the psychological impact generated by the pandemic, has diverted employees' attention from data security and hardware protection practices, creating significant cyber bio vulnerabilities to the life science enterprise.

As critical security flaws grow, attacks become more widespread and aggressive, posing risks to intellectual property and fraud across all areas of the bio-economy. Concerning trends in privacy and

[137] Schneier B, 'Securing Medical Research: A Cybersecurity Point of View', (*Science*, 2012), 336(6088), pp. 1527-1528.

[138] Cebo D., 'Strategical Analysis of Cyberbiosecurity in 2022: How to Defend Biotech and Healthcare Sector from Cyber Treats', (2022), p.5.

digital ethics that are being largely debated look even more pressing in biological research, where the data collected is undoubtedly more sensitive.

Mounting concerns are specifically relevant to those countries lacking adequate biotech, medical and cyber-infrastructures and thus labelled incapable of protecting their populations from technological threats. Indeed, if globalization has hastened the transmission of know-how and technological expertise worldwide, it has equally multiplied security vulnerabilities moving beyond physical borders. As effectively summed up by US President Biden "*many of the biggest threats we face respect no border or walls*" [139].

The spillover of cyber dangers to the physical space is raising unprecedented concerns over cyber-bio security and bio safety, exposing public health and the environment to unknown hazards.
Besides attacks on hospitals, genomic databases, and supply chains, the more dangerous include engineered pathogens that reproduce common disease symptoms or provoke fatal immune systems events. As complementary pillars of international health security, biosecurity is referred to in the Biological Toxin Weapons Convention[140] (BTWC) as "*security-enhancing mechanisms to establish and maintain the security and oversight of pathogenic microorganisms, toxins and relevant resources*"[141], while biosafety broadly deals with preventing the unintentional exposure to infectious agents, or their accidental release from research laboratories.

This trend is clearly illustrated by the dual use of Synthetic biology (SynBio) advances. Broadly described as an integrated discipline of biology and engineering, its application allows "*the design and construction of novel artificial biological pathways, organism or devices, or the redesign of existing natural biological systems*"[142].
As such, bioinformatics tools provide researchers with the capability of manipulating and designing living cells in a virtual habitat, obtaining non-natural DNA sequences. While driving far-reaching improvements in biomedicine and health, it poses potential biosecurity risks, urging the attention of researchers and policymakers.

Likewise, laboratory safety represents a hot topic of the 21st century. Advances in laboratory automation have made access to research equipment easier than ever before, increasing simultaneously concerns over privacy, data protection, and other principles including transparency,

[139] Schmidt T., 'What the President's Interim National Security Strategic Guidance means for the U.S. Military', (*The Pacific Council magazine*, 2022).
[140] United Nations, 'Convention of the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction', New York, (1971), 1015 UNTS, entry into force 26 March 1975.
[141] Domingo J, 'The Biological Weapons Convention (BWC) And Biosafety Diplomacy', (*Applied Biosafety*, 2008),13(2), pp. 1-3.
[142] Li J. and others, 'Advances in Synthetic Biology and Biosafety Governance', (*Frontiers in Bioengineering and Biotechnology*, 2021), 9, pp. 2.

accountability and equity. Undoubtedly, the dual-use potential of technological innovation makes their regulation rather difficult.

Once limited to trained laboratorians, the potential of an automated laboratory is now sold as commercial biological production facilities which may unintentionally generate components of high impact biological agents.

Thus, the openness and transparency of the scientific community might fall victim to exploitation. "*Within intelligent and connected biolabs, each point in the automated process has cyber and biosecurity vulnerabilities that could be hacked*"[143], potentially undermining any of the pillars within the CIA triad, namely, Confidentiality, Integrity and Availability.

Besides disturbing the ecological balance if accidentally released, genetically engineered microorganisms can be used as "*a substrate to inject malware into a computer system*"[144].

The increasing accessibility of genomic databases allows attackers with enough expertise to easily encode genetic sequences, control them remotely and weaponize the output. Advances and applications are thus easily accessible for malicious actors who can get all necessary components to produce toxins or pathogens without having to acquire them from a company or a lab or undergo mandatory checks and investigations.

Fuelled by declining costs of gene-editing tools, the practice of biohacking is increasingly performed by amateur biohackers outside institutional laboratories, potentially leading to illegal substance manufacturing and unregulated genetic enhancements.

The manipulation of medical data, along with cyberattacks on biomanufacturing causes serious economic and social costs. Yet, the most enduring impact will be on citizen's trust in critical infrastructures, public health institutions and data-systems. As SynBio capabilities and techniques mature and diffuse, barriers to the acquisition of emerging technologies reduce, providing hostile states and non-state actors with new opportunities to develop rather inexpensive biological weapons.

Overall, advances in information and communication technology are transforming the nature of warfare, pointing to a world where international relations are extremely uncertain. As a result, the concept of security itself is continuously developing, involving different dimensions and levels.

The unique risks coming from biological advances require a proactive approach. The diversity of jurisdictional and cultural value systems makes national responses insufficient.

[143] Pauwels E., 'The New Geopolitics of Converging Risks: The UN and Prevention in the Era of AI' (*United Nations University Centre for Policy Research*, 2019), p.27.

[144] Peccoud J, and others, 'Cyberbiosecurity: From Naive Trust to Risk Awareness', (*Trends in Biotechnology*, 2018), 36(1), p.4.

Chapter 2

The law governing cyber-warfare and cyberspace in the international and European context: an analysis of normative gaps

2.1. Cyber-warfare and the applicability of the international humanitarian law

Over the last decades, the pervasive development of information and communication technologies (ICTs) providing continuous access to sensitive data has resulted in increasing episodes of unlawful activities, through Cyber Information Operations (IO). Otherwise known as influence operations, they imply the use of information-related capabilities to disable adversaries' information systems infrastructure and vital services to communities[145].

Increased access and connectivity have multiplied security vulnerabilities, transforming cyberspace into an increasingly critical battleground. Besides institutions and governments, cyberspace's governance has emerged also among individuals and private actors who have designed Internet infrastructures and defined technical and legal standards, consequently contributing to the rise of ICT companies, whose platforms have however offered fertile ground for hostile cyber behaviours[146]. It has followed an increasing State's interest in exploiting cyberspace as a zone for geopolitical rivalries[147].

Thereby, the governance of cyberspace involves a set of stakeholders, that is not merely limited to States. However, since international law governs primarily relations among states, regulations on cyberspace fall outside its monopoly[148]. As numerous players from industry and society are involved, other regulatory systems apply[149].

Nowadays, most infrastructures – including banking and financial systems, telecommunication and transport networks, electrical grids, water supplies and emergency services – are largely controlled by computer networks and information technology solutions, turning into a major target for malicious activities[150]. Alarmingly, cyberattacks have challenged the understanding and application of

[145] Gillam M. M., 'Information Warfare: Combating the Threat in the 21st century', (1997), pp.2-4.
[146] The 1990s brought an explosion of cyber virus infecting millions of users worldwide. Common attack techniques include spyware, phishing, Distributed Denial-of-Service (DoS), Trojan horses and numerous more.
[147] Riordan, S., 'The Geopolitics of Cyberspace: A Diplomatic Perspective', (*Brill Research Perspectives in Diplomacy and Foreign Policy*, 2018), 3(3), pp.32-34.
[148] Marks S., 'State-Centrism, International Law, and the Anxieties of Influence', (*Leiden Journal of International Law*, 2006), pp. 339–347.
[149] Klimburg A. and Faesen L., 'A balance of Power in Cyberspace', (*The Hague Centre for Strategic Studies*, 2022), pp. 7-8.
[150] Dunn Cavelty M. and Wenger A., *Cyber Security Politics Socio-Technological Transformations and Political Fragmentation*, (Routledge, 2022), pp. 4-6.

International Humanitarian Law (IHL)[151], empowering numerous organisations to "exploit" existing legal gaps[152].

Traditionally, emerging conflicts between nations have been governed by the law of armed conflict, regulating the conduct of hostilities between belligerent parties. The spontaneous emergence of terrorists, hacktivists and other non-traditional actors in the international arena has made it unclear how to react and what consequences might apply.

Although the application of (general) international law in cyberspace has been widely accepted, laws and policies governing the use of force have revealed inadequate to face the current international system, giving rise to a debate especially around the attribution issue[153].

In International Humanitarian Law (IHL) attribution is defined as "*the means by which responsibility for illegal acts or omissions are attached to the state*"[154], distinguishing between the concept of both direct and indirect responsibility. It follows that States are liable for wrongful acts or omissions conducted officially by their *de jure and de facto* state agents[155]. It is consequently required to ascertain the identity of whoever is accountable for the conduct in question before applying international law in cyberspace.

In identifying the perpetrator of an attack, security analysts start tracking down the exact location from where the attack was carried out, whom the software was designed by and the reasons for its design. Answering all these questions isn't as easy as it might look. The rapid expansion of the Internet, together with the increasing hackers' capabilities of hiding and faking information, make it particularly difficult for intelligence analysts to investigate incidents and identify the origins of malicious behaviour. Attribution gets even harder when states employ proxies, whose evidence of control is rarely obtained[156].

Consequently, due to technical difficulties in ascertaining the attribution of a wrongful act related to cyberspace, States tend to frequently use public attribution – regardless of any clear legal basis[157] ,

[151] International Humanitarian Law, *i.e.* the law of armed conflict or the *jus in bello*, is the legal framework regulating the use of violence in situations of armed conflict, thus defining principle and responsibilities for States and non-States actors during armed conflicts.

[152] Diamond E., 'Applying International Humanitarian Law to Cyber Warfare', (*Institute for National Security Studies*, 2014), pp. 70-77.

[153] Assumpção C., 'The Problem of Cyber Attribution Between States', (*E- International Relations*, 2020), pp. 1-6.

[154] Grosswald L., 'T Cyberattack Attribution Matters Under Article 51 of the U.N. Charter', (*Brooklyn Journal of International Law*, 2011), 36(3), pp. 1154.

[155] *De jure* agents generally include government personnel and persons designated as State agencies legally empowered to act on behalf of the State and exercise governmental authority. *De facto* agents, instead, comprise both private persons or groups acting under the control and direction of a State and persons exercising security or military functions with no legal authorization.

[156] Hutchins G. S. Pirolli L. P. and K. Card K.S., 'What Makes Intelligence Analysis Difficult? A Cognitive Task Analysis of Intelligence Analysts', (*Calhoun*, 2007), pp.8-11.

[157] Levite A, Chuanying L. Perkovich G. and Yang F., 'Managing U.S.-China Tensions Over Public Cyber Attribution', (*Carnegie*, 2022), pp. 7.

while little of them favour cooperative coalitions aiming at establishing state accountability as per applicable international law.

As a result, widespread non-compliance with international law has become a serious impediment, and it has even encouraged the private sector to fill in the legal vacuum, driving and shaping new norms in digital defence. This phenomenon has grown uncoordinated, building new rules of cyberspace behaviour clashing with States' interests[158].

A second critical issue implies the concept of 'authority'. The question raised runs around the extent to which IHL is legally empowered to impose law in cyberspace. Although the content of the IHL has been widely accepted by the international community, its authority on states is rather questionable[159]. Despite its binding nature for nations publicly accepting it, the lack of centralised authority makes "*both international law and international legal procedures either ignored by states or distorted by the parties to further their own interest*"[160]. This becomes even harder when applied to non-state actors involved in cyber-attacks.

Also, what is subject to debate is the question of whether cyber-attacks constitute an unlawful use of force[161]. The answer assesses IO activities and defines whether they fall below the threshold of the UN Charter, which in turn clarifies what countermeasures can be implemented.

Particularly noteworthy is Article 2(4) which articulates that "*all members [of the United Nations] shall refrain in their international relations from the threat or [armed] use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations*"[162]. Accordingly, unless a valid reason is envisaged in international law, the use of force and the threat of it are both prohibited.

Only two exceptions apply to the mentioned rule. First, forceful measures are authorized by the Security Council when deemed "*necessary to maintain or restore international peace and security*"[163]. The second legal justification refers to "*the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations*"[164]. In other words, a state is legally entitled to embark upon the use of armed force when it falls victim to an armed attack or

[158] Hoffman W. and Levite A., 'Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?' (*Carnegie*, 2017), pp. 13-18.
[159] Kelley M., 'Challenges to Compliance with International Humanitarian Law in the Context of Contemporary Warfare', (*Independent Study Project*, 2013), pp.7-8.
[160] Mills, I., 'Emergent International Humanitarian Law in the Context of Cyber Warfare', (*Journal of Film and Media Studies, 2017)*, 2(1), pp.78-99.
[161] Buchan R., 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? ', (*Journal of Conflict & Security Law*, 2012), 17(2), pp. 211-227.
[162] United Nations, 'Charter of the United Nations', San Francisco, (1945), 1UNTS XVI, Art. 2(4).
[163] Ibidem, Chap. VII, Art.42.
[164] Ibidem, Art. 51.

when it acts to assist another attacked State. It follows that the law of armed conflict applies when a state exceeds the threshold limit, legitimizing reprisals as counter-instruments.

The tricky issue lies in what is defined under Article 51 as 'an armed attack', which identifies a narrower sector of actions than the 'use of force' and it usually involves some sort of physical or human damage. Customary law – as clarified by the International Court of Justice (ICJ) in the *Nuclear Weapons Advisory Opinion* - advises that Article 2(4) covers "*any use of force, regardless of the weapons employed*"[165]. A similar approach is expressed in the so-called Martens Clause which made its first appearance in the preamble of the 1899 *Hague Convention II*[166] and was then renewed in article 1(2) of the *Additional Protocol I to the Geneva Conventions*[167]. The mentioned clause states that "*in cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience*"[168]

Overall, the lack of a definition requires a good faith in interpreting an 'armed attack' (or the commencement of it) in compliance with the Charter's object and purpose[169]. Although the Additional Protocol I to the Geneva Conventions specifies under Article 36 that states developing new techniques of warfare have the responsibility to declare whether their use would be prohibited[170], different understandings of the term have raised and continue to evolve in response to changing threats and situations[171].

Through the *travaux préparatoires*, it seems clear that under the UN Charter the prohibition of force doesn't include political and economic coercion[172]. Likewise, Article 41 mentions "*interruption of communication*" as a "*measure not involving armed force*"[173], implying that some cyber-attacks don't directly fall into the prohibition of Article 2(4). The lack of direct violent effects must not make one think that cyber operations fall outside the scope of armed force, notwithstanding the lack of

[165] International Court of Justice (ICJ), 'Legality of the Threat or Use of Nuclear Weapons: Advisory Opinion', Hague, (1996), para. 39.
[166] International Committee of the Red Cross (ICRC), 'The Hague Conventions of 1899 (II): Respecting the Laws and Customs of War on Land', Hague, (1915), entry into force 9 September 1900.
[167] International Committee of the Red Cross (ICRC), 'Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)', Geneva, (1978), entry into force 7 December 1979.
[168] Ibidem, Art. 1(2).
[169] United Nations, 'Vienna Convention on the Law of Treaties', Vienna, (1969), 1155 UNTS 331, entry into force 27 January 1980, Art. 31(1).
[170] Ibidem, Art.36.
[171] Upeniece, V., 'Conditions for the lawful exercise of the right of self-defence in international law', (*SHS Web of Conferences*, 2018), pp.5-6.
[172] Amerasinghe, C., 'The Charter Travaux Préparatoires and United Nations Powers to Use Armed Force', (*Canadian Yearbook of International Law*,1966) ', 4, pp. 81-101.
[173] United Nations, 'Charter of the United Nations', San Francisco, (1945), 1 UNTS XVI, Art. 41.

consensus on criteria defining the precise threshold at which cyberattacks must be considered prohibited under Article 2(4) of the UN Charter.

These controversies have offered States an opportunity to develop a practice related to cyberspace without a clear regime of international law applicable to the latter. This has caused a clear division of interpretations and standards, which have resulted in different national policies and practices determining when another state's actions represent an armed use of force, legally legitimizing a response in self-defence[174].

This confusion has led to the rise of the concept of the fifth-dimension warfare, distinguishing itself from the four other domains of warfare - land, sea, air and space[175].

Although many analysts believe IO can be regulated by analogy to the existing international law of war, numerous issues remain still unanswered. The ensuing analysis underscores the influence of cyberspace on international dynamics, opening the door to new challenges.

Overall, scholarly debates underscore the inadequacy of international humanitarian law in dealing with information operations. The greatest obstacle lies in the lack of consensus-building and negotiation across the international community, making it harder to interpret the law and define what the legal responses are.

2.1.1. The Tallinn Manual and international cyber security law

Cyber hacking and spying have encouraged both national states and multinational entities to find innovative solutions. Acknowledging the potential of cyber warfare, States have turned to proactive cyber defence measures, spawning a new structure of administrative governance.

On the international stage, the main effort was directed by the North Atlantic Treaty Organization (NATO) whose Cooperative Cyber Defence Center of Excellence (CCD COE) located in Tallinn, Estonia sought to define the original Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual 1.0)[176] and the newly published Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations[177], that ultimately engaged a broader international group of experts from Thailand, China, Japan, and Belarus. The content of Tallinn 2.0 is mainly built upon the

[174] United Nations, 'Charter of the United Nations', San Francisco, (1945), 1UNTS XVI, Art. 51; NATO Cooperative Cyber Defence Centre of Excellence, 'Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0', (2013), Rule 13.

[175] Kasapoglu C., 'Cyber Security: Understanding the Fifth Domain', (Centre for Economics and Foreign Policy Studies, 2017), pp. 1-3.

[176] NATO Cooperative Cyber Defence Centre of Excellence, 'Tallinn Manual on the International Law Applicable to Cyber Warfare 1.0', (2013).

[177] NATO Cooperative Cyber Defence Centre of Excellence, 'Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0', (2017).

first edition while expanding its coverage area to cover a broader spectrum of cyber activities and clarifying a few contentious points since its original publication.

Its non-binding nature is made clear in its introduction, stating that "*the Manual is meant to be a reflection of the law as it existed at the point of its adoption*"[178]. In other words, it objectively restates the legal doctrine of customary international law on the use of cyberweapons, heading to achieve a consensus on the *jus in bello* and the *jus ad bellum* applying to operations in and through cyberspace. Aware of the legal uncertainty governing such a grey area, the project suggests cyberspace activities be handled through international law under particular circumstances, raising numerous controversial issues.

As a core principle of international law, sovereignty applies to cyberspace, mirroring in rules prohibiting the use of force and intervention. In this regard, Rule 10 prohibiting whatever cyber operations constitute a threat or use of force[179] mirrors both the content of Article 2(4) of the UN Charter and reflects the customary international law. Despite this clarification, the scope of its application is still contested. As a customary rule, the prohibition rule applies both to members and non-members of the United Nations, while it leaves unhandled the conduct of entities that are not directly attributable to a national state.

This state-oriented approach creates a huge legal vacuum. Following the ICJ's ruling on the Nicaragua case[180] advising the indirect use of force falling inside Article 2(4), some commentators interpreted it extensively, covering judgemental activities of non-state actors[181]. Because their act violates the right of states "*to be free from the threat or use of force*"[182], it is believed it should be assessed under the customary prohibition on force[183].

A similar controversial topic relates to Rule 11, defining "*a cyber operation as a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force*"[184]. In other words, any force causing harmful effects amounting to those by military force is labelled as

[178] Ibidem, pag. 9-10.
[179] NATO Cooperative Cyber Defence Centre of Excellence, 'Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0', (2017), Rule 10.
[180] International Court of Justice (ICJ), 'Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America) ', (1986).
[181] Thomas M. Franck, 'Terrorism and the Right of Self-Defense' (*American Journal of International Law*, 2001), 95, pp. 839- 840; Schmitt M. and Watts S., 'Beyond State-Centrism: International Law and Non-state Actors in Cyberspace', (*Journal of Conflict & Security Law*, 2016), 21(3), pp. 595-611.
[182] Tsagourias N., 'Non-State Actors and the Use of Force', in D'Aspremont J., *Participants in the International Legal System: Multiple Perspectives on Non-State Actors in International Law* (Routledge, 2011), pp. 326.
[183] Ibidem.
[184] NATO Cooperative Cyber Defence Centre of Excellence, 'Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0', (2017), Rule 11.

prohibited. This effects-based approach raises the question of whether cyber operations with severe non-physical effects could be compared to use of "physical" force.

It seems the Manual makes cyber operations fall outside the meaning of Article 2(4), by ignoring economic or political coercion under the notion of force[185]. Cyberattacks may nevertheless look rather serious when affecting states' economic and political wealth, without necessarily translating into physical damage.

On closer look, the Manual doesn't take a categorical position on the aforementioned issue. When discussing how to assess a cyber force as unlawful for Article 2(4), the Manual specifies a *de minimis* threshold of 'scale and effects', advising a number of factors to take into account – notably "*immediacy, invasiveness, severity, directness, state involvement, measurability of effects, presumptive legality and military character of the operation*"[186]. That said, although the inclusion of these factors offers a policy evaluation perspective, the list is neither exhaustive nor binding[187].

These assumptions must not let one think that all acts falling outside the meaning of Article 2(4) are legally accepted. They may amount to what is recognized as an unlawful intervention which covers any dictatorial and coercive interference in another state's affairs[188]. Hence, for a certain cyber operation to be assessed as an unlawful intervention, it requires to be attributed to a state, which, as seen above, is rather difficult in cyberspace. This has opened the door to plenty more questions which remain still unanswered.

To mention a few, the first issue regards whether non-state actors' conduct not attributable to a state is covered in the definition of unlawful intervention, while the second question concerns whether a non-state' activities falling below *the minimis* threshold imposed in article 2(4) match the idea of unlawful intervention.

The definition of the threat of force addressed in Rule 12 - drawing on the ICJ's definition outlined in its *Nuclear Weapons* Advisory Opinion[189] - is far from clarity and consensus.

The first concern is about the legality of certain applications of force, as during humanitarian assistance operations. A second issue questions the broad conception of self-defence rights and whether they include cyber force as countermeasure purposes. In this regard, the lack of clarification on how to measure the gravity of an attack makes any determination challenged.

---

[185] Tsagourias N., 'The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II—The Use of Force' in Terry D. Gill, *Yearbook of International Humanitarian Law*, (Springer, 2014), pp.22.

[186] NATO Cooperative Cyber Defence Centre of Excellence, 'Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0', (2017), Rule 11, Para. 9.

[187] Ziolkowski K. 'Jus ad bellum in Cyberspace – Some Thoughts on the ''Schmitt-Criteria'' for Use of Force', (NATO CCD COE Publications, 2012). Available at: <http://www.ccdcoe.org/publications/2012proceedings/5_3_Ziolkowski_IusAdBellumInCyberspace.pdf>, (accessed 7 July 2022).

[188] Jennings R., and Watts A., *Oppenheim's International Law*, (Oxford, 2008), pp. 432-439.

[189] International Court of Justice (ICJ), 'Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion', Hague, (1996), para. 47.

In many cases, the historical, political and military context is to take into account when assessing a particular conduct, which explains why the understanding of this matter is rather ambiguous.
A similar pressing issue relates to the UN Charter's statement "*or in any manner inconsistent with the purposes of the United Nations*"[190] which extends the meaning of threats or uses of cyber power beyond the mere acts against the political defence or territorial integrity of a State. As the UN is guided by numerous purposes, including security, peace, and protection of human rights, an all-inclusive approach is highly debated[191].

Following the Manual's launch, one area of particular concern has been the due diligence obligation towards potential wrongful cyberattacks, addressed in Rules 6 and 7. The mentioned rules uncontestably acknowledge the States' responsibility to apply due diligence as part of international law. In particular, States are called to prevent and avoid their cyber infrastructures to be maliciously exploited for cyber operations, potentially causing serious adverse consequences[192]. Yet, what they meant by 'serious adverse consequences' is not sufficiently described. Also, when a State is notified of potential transboundary harm, it is expected to adopt "*all measures that are feasible in the circumstances to put an end to the cyber operations*"[193]. Yet, because of the difficulties in allocating responsibility, States are rather reluctant to engage in due diligence, which is mostly deemed to be resource-intensive[194].
Predictably, the protection of human rights in cyberspace has arisen the most disagreement among experts[195]. Although there is no consensus on a list of human rights strictly related to cyberspace, some of them are distinctly important, namely the rights to freedom of opinion, expression, due process and privacy.
While acknowledging the non-derogability of certain fundamental human rights, it is noteworthy that the right to privacy is subject to limitations, as expressed in rule 37 which states "[*t]he obligations to respect and protect international human rights, with the exception of absolute rights, remain subject to certain limitations that are necessary to achieve a legitimate purpose, non-discriminatory, and*

[190] United Nations, *Charter of the United Nations*, San Francisco, (1945), 1 UNTS XVI, Art.2 (1).
[191] Talbot Jensen E., 'The Tallinn Manual 2.0: Highlights and Insights', (*Georgetown Journal of International Law*, 2017), pp.775-776.
[192] NATO Cooperative Cyber Defence Centre of Excellence, 'Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0', (2017), Rule 6.
[193] NATO Cooperative Cyber Defence Centre of Excellence, 'Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0', (2017), Rule 7.
[194] Yuying Liu I., 'The due Diligence Doctrine under Tallinn Manual 2.0', (*Computer Law & Security Review*, 2017), 33(3), pp. 390-295.
[195] Barnsby E.R. and Reeves R.S., 'Give Them an Inch, They'll Take a Terabyte: How States May Interpret Tallinn Manual 2.0's International Human Rights Law Chapter', (*Texas Law Review*, 2017), pp.1515-1530.

authorized by law"[196]. The greatest ambiguity lies around the concept of "legitimate purpose". Although the efforts to define legitimate criteria for measuring a legitimate cause, the list provided looks rather incomplete. For greater clarity, some examples are shown: "*protection of rights and reputations of others, national security, public order, public health, [and] morals*"[197]. Of major concern is the concept of "countering terrorism" which is stated as a legitimate purpose for States to monitor online activity and communications without defying the right to privacy. Although checks on potential abuses are provided, no further explanation is specified, which makes states able to exploit the exception of 'terrorism' and limit human rights.

The lack of a universally accepted understanding of the term 'terrorism' has caused a myriad of national and regional interpretations. The closest achievement has been the *United Nations Security Council Resolution* 1566[198]. Nonetheless, the vagueness around the definition allows a wide room of manoeuvre for States to determine what it implies. Likewise, the example of 'countering terrorism' as a 'legitimate purpose' seems to be very broad, which in turn risks being strategically and dangerously applied in a variety of circumstances, increasing the chances of abrupt limitations on international human rights.

Equally alarming is the ambiguity around the concept of 'public order', 'national security' or 'public health' as legitimate motives[199]. This has resulted in definitional gaps potentially being used to threaten IHRL over time

Overall, Tallinn 2.0's IHRL Chapter refers to foundational concepts with both ambiguity and vagueness, which consciously leaves space for further legal actions.

Although it marks a bold step forward in intersecting multiple areas of the law, the Tallinn Manual present some big concerns that confound legal scholar and policymakers. The project gathers some conclusions from experts that vary from barely sufficient to extremely scarce, offering mostly rough guidelines and barely resolving contentious matters[200].

In light of identified gaps, a five-year project has been recently launched to revise existing chapters and explore emerging topics. The non-legally binding nature of the Manual will remain unchanged while a broader community of researchers, analysts, industry and civil society players will be

[196] NATO Cooperative Cyber Defence Centre of Excellence, 'Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0', (2017), Rule 37.
[197] Ibidem.
[198] UN Security Council, 'Security Council resolution 1566 concerning threats to international peace and security caused by terrorism', (2004), S/RES/1566.
[199] NATO Cooperative Cyber Defence Centre of Excellence, 'Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0', (2017), Rule 37(5).
[200] Cong W., 'Seeking Customary International Human Rights Law in the Cyberspace: A Critique of the Tallinn Manual 2.0', (2018), Available at SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3744924>, (accessed 9 July 2022); Colin P., 'Debugging the Tallinn Manual 2.0's Application of the Due Diligence Principle to Cyber Operations', (*Washington International Law Association*, 2019), 28(2), pp. 597-604.

involved in updating the chapters of the Manual, addressing evolving cyber security threats and current States practices[201].

2.1.2. The Budapest Convention on Cybercrime and its key components

The growing threat of cybercrime and its translational nature has urgently called out for a multilateral instrument regulating and harmonising cybercriminal practices. Nationally, cybercrime was barely approached or at best partially covered in laws prohibiting offline crimes.

Acknowledging the lack of a cohesive approach, the Council of Europe convoked a working group from which the Convention on Cybercrime[202] - also known as the Budapest Convention – originated. The Committee was entrusted with the task of defining a common approach to international cooperation in the matters of "*jurisdiction and data exchange in terms of the investigation of cyber-space offending*"[203], serving as a benchmark for national legislations. Adopted in 2001, it finally entered into force a few years later requiring signatories to introduce appropriate rules and cooperative practices to adequately protect societies against cybercrime.

The Convention[204]'s greatest limitation lies in the little participation of countries worldwide[205], limiting its influence and impact to only 66 countries that ratified it[206]. Russia publicly declared the treaty as being in violation of its national sovereignty[207], while India declined to adopt it as it was not involved in the drafting of the Convention itself [208]. Also, many Latin American countries refused to sign the treaty, which overall suggests the little value of a European Convention for the rest of the world, leaving broad swaths of the globe outside the Convention's control.

[201] 'CCDCOE To Host The Tallinn Manual 3.0 Process' (*Ccdcoe.org*, 2022), Available at: <https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/>, (accessed 9 May 2022).
[202] Council of Europe, 'Convention on Cybercrime', Budapest, (2000), ETS 185, entry in force 1 July 2004.
[203] Council of Europe, 'Explanatory Report to the Convention on Cybercrime', Budapest, (2001), ETS 185, para.3.
[204] Composed of four main sections, the treaty deals with numerous topics ranging from frauds and attacks on technology-based networks, to investigation and prosecution procedures for online crimes and cooperative measures for the exchange of evidence between partner entities.
[205] Most Council of Europe treaties are open for accession by non-member States, including non-European countries.
[206] Council of Europe, 'Chart of Signatures and Ratifications of Treaty 185' (*Coe.int*, 2022), Available at: <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185>, (accessed 10 May 2022).
[207] 'The Hypocrisy of Russia's Push for a New Global Cybercrime Treaty' (*Lowyinstitute.org*, 2022), Available at: <https://www.lowyinstitute.org/the-interpreter/hypocrisy-russia-s-push-new-global-cybercrime-treaty>, (accessed 11 May 2022).
[208]Vipul Kharbanda, 'International Cooperation in Cybercrime: The Budapest Convention — The Centre for Internet And Society' (*Cis-india.org*, 2019), Available at: <https://cis-india.org/internet-governance/blog/vipul-kharbanda-april-29-2019-international-cooperation-in-cybercrime-the-budapest-convention>, (accessed 11 May 2022).

Failing to receive the support of African countries - with the exception of South Africa and Senegal, two-thirds of the world continues to chart its own route[209].

One of the main obligations signatories countries are called for is the enforcement of substantive criminal provisions unifying domestic cyber laws. Cultural differences among nations are however the greatest obstacle to achieving harmonization in the area. Each States has indeed is own understanding of what criminality is and the rights granted to the accused. In an effort to reach a common ground, the CoE Convention has adopted a flexible harmonization paradigm, leaving "*the formulation of procedural due process rules to the cultural peculiarities of each nation*"[210]. Law enforcement is thus confined to national authorities, which are increasingly reliant on foreign counterparts' cooperation. Long-standing inconsistencies among cyber national laws, however, hinder the real success of international criminal prosecutions and mutual assistance activities.

First, although criminalization requirements are exhaustively covered in the CoE Convention, not all listed offences[211] are codified as illegal, leaving the issue on domestic interpretations. Besides, adequate resources and procedural tools are required to conduct successful criminal investigations, which, however, many States lack. Yet, even when both requirements are fulfilled, the lack of enforceable cooperation hampers the prosecution's process. In this regard, one cannot but recognize the superiority of national laws and their implementing systems at the national level.

The lack of a dual criminality provision[212] is, however, feared to endanger due process, mutual assistance and human rights protection. As stated in article 25 (4) of the Convention "*mutual assistance shall be subject to conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation*"[213]. It translates into the freedom of states to apply traditional methods to assistance requests. Hence, dual criminality applies when provided by national laws or other international agreements. Major steps forwards mostly come from other international mutual assistance treaties,

[209] Clough J., 'A World of Difference: The Budapest Convention on Cybercrime and The Challenges of Harmonisation', (*Monash University Law Review*, 2013), 40(3) pp.700-701.

[210] Miquelon-Weismann M., 'The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process? ', (*Journal of Computer and Information Law*, 2005), 23(2), pp. 342.

[211] The core offences are illegal access and interception (respectively in Art.2 and 3), system and data interference (respectively treated in articles 5 and 4), misuse of devices (Art.6), computer-related offences (Art.8) and content-related offences (Art.9).

[212] The principle of double criminality *"holds that an act is not extraditable unless it constitutes a crime in both the requesting and requested countries".*
Bernholz S.A., Bernholz M.J.,Herman G.N., 'Problems of Double Criminality', (*Trial*, 1985), 21(1), pp. 58-63.

[213] Council of Europe, 'Convention on Cybercrime', Budapest, (2000), ETS 185, entry in force 1 July 2004, Art. 25(4).

such as the *European Convention on Mutual Assistance in Criminal Matters* (1959)[214] and the *United Nations Convention on Transnational Organized Crime* (2001)[215].

The Convention wording is rather vague, which has opened to various interpretations. While some scholars suggest it was purposely made, leaving some space for either improvement or development, laws might progressively deteriorate becoming totally ineffective to face evolving online crime[216]. For instance, when dealing with investigative powers the greater concern is the lack of clarity in listing the kind of offences potentially subject to the mentioned powers, which may automatically be applied to any serious or minor offences.

The most relevant criticism refers to the old-fashioned approach to cybercrime that looks at offending - in a traditional way - as targeting society and causing harm. Yet, what it misses is the evolving nature of the online crime threat that invisibly overcomes borders. The wording in Article 32 (b) referring to "*stored computer data located in another Party*"[217] suggests that data's location is generally noted. Yet, modern advances show things have radically changed, with data dynamically shifting among jurisdictions.

What is mostly objected is its attitude to the protection of state and individual rights[218]. Here, the difficulties of harmonisation become even greater as the bipolar need to both improve law enforcement and protect individual freedoms and privacy results in evident tensions.

Given the broadness of legal systems and cultures involved, the Convention adopt a pragmatic approach, requiring states to apply appropriate protections and standards drawing both upon domestic and international law[219] - under the *Convention for the Protection of Human Rights and Fundamental Freedoms* (ECHR)[220] and the *International Covenant on Civil and Political Rights* (ICCPR)[221], as well as "*other applicable international human rights instruments*"[222].

This becomes evidently problematic for those countries that have not ratified the mentioned international instruments, which may result in less human rights protection in practice. This, however,

[214] Council of Europe, 'European Convention on Mutual Assistance in Criminal Matters', Strasbourg, (1959), ETS 30, Art.5 (1a), entry into force 12 June 1962.
[215] UN General Assembly, 'United Nations Convention against Transnational Organized Crime: resolution / adopted by the General Assembly', (2001), A/RES/55/25, Art 18(9).
[216] Baron R., 'A Critique of the International Cybercrime Treaty', (*Journal of communications law and policy*, 2002), 10(1), pp. 271-273.
[217] Council of Europe, 'Convention on Cybercrime', Budapest, (2000), ETS 185, entry in force 1 July 2004, Art.32(b).
[218] Clough J., 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation', (*Monash University Law Review*, 2013), 40(3), pp.708.
[219] Ibidem.
[220] Council of Europe, 'European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14', Rome, (1950), ETS 55, entry into force 3 September 1953.
[221] UN General Assembly, 'International Covenant on Civil and Political Rights', New York, (1966), UNTS 999, entry into force 23 March 1976.
[222] Council of Europe, 'Convention on Cybercrime', Budapest, (2000), ETS 185, entry in force 1 July 2004, Art. 15(1).

doesn't originate from the inherent functioning of the Convention itself, but rather from the process of accession. In particular, applicant countries can accede to the Convention only by invitation[223], which is not however followed by a review of the existing human rights standards. This, in turn, discourages the uptake of robust requirements. The recent accession of Tonga, in May 2017[224] is an outstanding example in this respect[225].

Some commentators have expressed some doubts about the flexibility of the present approach as it sounds like "*a model of uniform rule-making confined to establishing parameters for acceptable substantive rules, leaving the formulation of procedural due process rules to the cultural peculiarities of each nation*"[226].

While this helps law enforcement achieve its objectives, it might damage the concepts of due process and the preservation of individual rights as no specific minimum standards are provided[227].

Of much concern is the concept of privacy which is barely addressed in Article 15, stating that the "*implementation and application of the powers and procedures provided are subject to conditions and safeguards under domestic law, which shall provide for the adequate protection of human rights and liberties*"[228]. The concepts of adequate protection and procedural conditions are not, however, fully unfolded, entrusting domestic instruments to specify more detailed requirements[229].

This strategy lying on the decentralisation of international law is not exclusive to the Convention at issue.

For instance, the Geneva Declaration of Principles and Plan of Action[230] stresses countries' responsibility to achieve common goals referencing international human rights law as an external benchmark, while complying with national differences.

Likewise, much debated is the lack of protection of states' rights. The cross-border nature of modern communications raises concerns over the multiple jurisdictions to deal with when accessing data.

---

[223] Ibidem, Art.37.

[224] Council of Europe, 'Tonga Joins the Budapest Convention on Cybercrime' (*Coe.int*, 2017), Available at: <https://www.coe.int/en/web/cybercrime/t-cy-news/-/asset_publisher/GxUcENEFhivB/content/the-kingdom-of-tonga-today-acceded-to-the-budapest-convention-on-cybercrime-to-become-the-55th-party-to-this-treaty-?inheritRedirect=false>, (accessed 13 May 2022).

[225] Besides not having ratified the ICCPR, the newly member country lacks data protection laws, and it is not even legally bound to introduce any changes, which has raised relevant queries.

[226] Miquelon-Weismann M., 'The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process? ',(*John Marshall Journal of Computer and Information Law*, 2005), 23(2), pp. 354.

[227] Ibidem, pp. 355-456.

[228] Council of Europe, 'Convention on Cybercrime', Budapest, (2000), ETS 185, entry in force 1 July 2004, Art. 15.

[229] Clough J., 'A World of Difference: The Budapest Convention on Cybercrime and The Challenges of Harmonisation', (*Monash University Law Review*, 2013), 40(3) pp. 719-720.

[230] The World Summit on the Information Society, 'Geneva Declaration of Principles and Plan of Action', Geneva, (2003), WSIS-03/GENEVA/DOC/4-E.

Although Law Enforcement Agencies (LEAs) are charged with conducting transborder searches, their conduct might compromise citizens' fundamental rights. Generally speaking, it would be considered a violation of territorial sovereignty when a State undertakes investigations outside its territory without a prior authorization of the concerned State.

Cross-border searches are however allowed in two cases: the first is that a Party and its competent authorities may access publicly available data, regardless of the evidence's location[231]. It follows the rights of LEAs to retrieve open data as any other public member, without asking for mutual legal assistance. The second is that a party can "*access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system*"[232].

Mostly contested is the breadth of the present provision which supposes permission must be voluntarily given. Accordingly, LEAs are authorized to communicate with foreign citizens and persuade them to provide the necessary authorization, potentially violating a state's sovereignty[233].

Overall, although the Convention offers a remarkable benchmark for the harmonisation of cybercrime laws, it still presents numerous critical issues to be addressed.

Recently, a new additional protocol to the Budapest Convention on Cybercrime[234] reshaping procedures for accessing digital data in the context of criminal investigations has been approved.

The Protocol has immediately raised disappointment because its inadequacy for protecting fundamental rights, especially those of endangered journalists, activists and technology users across the globe[235].

On this matter, the European Digital Rights association (EDRi), with other allies, expressed concerns about the compatibility of the Second Additional Protocol with the EU Treaties as well as with the European Charter of Fundamental Rights, urging the European Parliament to exercise the power

---

[231] Council of Europe, 'Convention on Cybercrime', Budapest, (2000), ETS 185, entry in force 1 July 2004, Art. 32(a).

[232] Ibidem, Art. 32 (b). This provision has been publicly objected to by Russia which saw it as a threat to the security and sovereignty of member countries.

[233] Clough J., 'A World of Difference: The Budapest Convention on Cybercrime and The Challenges of Harmonisation', (*Monash University Law Review*, 2013), 40(3) pp. 719-720.

[234] Council of Europe, 'Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence', Strasbourg, (2022), ETS 185.

[235] Despite the comprehensive recommendations proposed by the civil society during the process, they were not finally included in the final draft.
Global Civil Society, 'Submission to the Council of Europe, Comments and suggestions on the Terms of Reference for drafting a Second Optional Protocol to the Cybercrime Convention', (2017), pp.8-13, Available at: <https://edri.org/files/surveillance/cybercrime_2ndprotocol_globalsubmission_e-evidence_20170908.pdf>, (accessed 14 May 2022).

provided under Article 218(11) of the Treaty of the Functioning of the EU (TFEU)[236] to ask the Court of Justice of the EU (CJEU) for a legal opinion[237].

Three main areas of concern have been expressed so far. First of all, the little feasibility to manoeuvre and reject direct requests looks rather critical for the protection of fundamental rights and certain safeguards in the criminal procedure law, *i.e.* immunities, privileges and special protections. Secondly, although the CJEU has established Law Enforcement Agencies' access to personal and private information to be bound to prior scrutiny by a court or an independent authority[238] – with the exception of specific urgent circumstances - the Protocol doesn't expressively provide this guarantee. The third major weakness is the lack of measures ensuring the Protocol's compatibility with the Court's requirements of essential equivalence, which undermines the level of individuals' rights protection.

Overall, the Budapest Convention represents a significant step forward in shaping a new corpus of international law in the response to cybercrime. Yet, numerous challenging issues have been raised since, questioning its real long-term effectiveness.

2.2. The EU regulatory framework on cybersecurity

Over the last decades, cybersecurity has become a keystone of a digital and connected Europe. The rapid spread of information and communication technologies, along with the widening of the European Union, has urged the extension of sectoral information security policies into a more inclusive cybersecurity framework ranging from technological sovereignty and resilience to cyber defence capabilities and responsible behaviour in cyberspace[239].

Although the second half of the 90s has marked the dawn of EU activities in electronic communication and computer security, the advancement of "*a fully-fledged strategy to cybersecurity*"[240] has taken a few decades before it was officialised.

As suggested by George Christou, one of the main factors pushing the EU to enhance its approach to cyber security lies behind the 2007 distributed denial of service (DDoS) attacks targeting Estonian

[236] European Union, 'Consolidated version of the Treaty on the Functioning of the European Union', (2009), 2008/C 115/01, Art. 218 (11).
[237] European Digital Rights, 'Ratification by EU Member States of the Second Additional Protocol of the Council of Europe Cybercrime. Convention Why is the opinion of the Court of Justice of the European Union necessary? ', (*EDRi*, 2022), pp.2.
[238] CJEU, 'Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems', CJEU - C-311/18, (2018).
[239] Kasper, A., Osula, A. and Molnár, A., 'EU cybersecurity and cyber diplomacy. (*IDP Revista de Internet Derecho y Política*', 2021), 34, pp.1-15.
[240] Carrapico, H.; Barrihna, A., 'European Union cyber security as an emerging research and policy field' (European Politics and Society, 2018), 19(3), pp. 299- 303.

businesses, public institutions and infrastructure, followed by a proliferation of offensive cyber security attacks at the EU and at the national level[241].

The perception of terrorism threats exploiting current gaps between Member States' laws has resulted in the development of a comprehensive legal, policy, and institutional framework encompassing all of the EU's core policy areas, including cybercrime and cyber defence. A joint and common approach has been progressively developed, following the inadequacy of national governments to deal with emerging transnational threats[242].

The first attempt to establish cybersecurity as a new EU policy area came in 2013, with the publication of the First European Union Cybersecurity Strategy – An Open, Safe and Secure Cyberspace (EU-CSS)[243] finally recognizing the convergence of three previously distinct areas: (*i*) critical infrastructure and information security – whose protection is well defined in EU law; (*ii*) privacy and data protection issues in electronic communications; (*iii*) cybercrime.

By establishing five main strategic priorities covering cyber resilience, cyber defence and cybersecurity issues, the 2013 Cyber Security strategy aims "to make the UE's online environment the safest in the world"[244], protecting the open Internet and promoting cyber cooperation with strategic stakeholders. Since then, the EU has actively contributed to multilateral forums, notably in the Open-Ended Working Group within the United Nations framework and in the UN Governmental Group of Experts[245], in enforcing cyber norms in the current international order.

A second important achievement in the EU's path towards a cyber policy is represented by the *Council conclusions on Cyber Diplomacy* adopted in 2015[246], when the Member States finally acknowledged the need for a coherent cybersecurity strategic framework while continuing multilateral dialogues with international and national key partners, both from the public and private sectors.

The multifaceted nature of cybersecurity encompasses numerous interlinked issues – namely human rights protection, internet governance, and the digital economy, all of them ruled by specific norms- has made the development of a cyber strategy a top priority. This fragmentation is perfectly entailed

[241] Christou, G., 'The collective securitisation of cyberspace in the European Union', (*West European Politics*, 2019), 42 (2) pp. 1-24.
[242] Luukas K. Ilves and others, 'European Union and NATO Global Cybersecurity Challenges: A Way Forward', (*Institute for National Strategic Security*, 2016), 6(2), 126-131.
[243] European Commission and HREU, 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', (2013).
[244] Viviane Reding, 'The EU's Data Protection Rules and Cyber Security Strategy: Two Sides of The Same Coin' (2013), Available at: <https://ec.europa.eu/commission/presscorner/detail/de/SPEECH_13_436>, (accessed 18 May 2022).
[245] It comprises of experts from 25 States studying on issues of concern and report observations and results at the UN General Assembly.
[246] General Secretariat of the Council, 'Council Conclusions on Cyber Diplomacy' 6122/15, Brussels, (2015).

in Ramses Wessel's saying who suggested cybersecurity forms "*an excellent example of an area in which the different policy fields need to be combined (a requirement for horizontal consistency), and where measures need to be taken at the level of both the EU and Member States (calling for vertical consistency)*"[247].

To achieve a solid and effective policy, a greater degree of coherence among Member States was thought to be needed, which was furtherly confirmed in the *2016 Implementation Plan on Security and Defence*[248].

The debate around the EU cybersecurity regulatory framework is strictly interrelated to the principle of conferral, under which the Union "*shall act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein*"[249]. In other words, EU legislative powers are generally performed in areas where the Union's intervention is considered more appropriate than the individual action of Member States, yet any legislative measure introduced at the EU level requires a legal basis falling under the conditions set out in Article 5 of the Treaty on European Union (TEU)[250]. Thus, a regulatory measure must fit into one of two categories to establish the Union's competence over a policy area: firstly, "*the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level*" or secondly, "*by reason of the scale or effects of the proposed action, be better achieved at Union level*"[251].

Given the above, and considering also the EU's little power on security matters, the European Commission provided justifications for new competencies in cybersecurity. This was finally accomplished in the *2016 Network and Information Security* (NIS) Directive[252] - whose revised version is currently under consultation[253] - highlighting a link between the increased digitalisation of the internal market and cybersecurity. The primary objective relates to the protection of critical, societal and economic infrastructures from cyber threats with "*a significant disruptive effect*"[254], guaranteeing "*a high common level of network and IT security*"[255] through multiple obligations upon

[247]Wessel R.A., 'Towards EU cybersecurity law: regulating a new policy field', in Tsagourias N., Buchan R. *Research handbook on international law and cyberspace*, (2015), pp. 500.
[248] High Representative of the Union for Foreign Affairs and Security Policy, Vice-President of the European Commission, and Head of the European Defence Agency, 'Implementation Plan on Security and Defence', 14392/16, Brussels, (2016).
[249] European Union, 'Consolidated version of the Treaty on the Functioning of the European Union', (2009), Art. 5.
[250] European Union, 'Treaty on European Union, Treaty of Maastricht', (1992), C 325/5, entry into force 1 November 1993.
[251] Ibidem, Art. 5(3).
[252] The European Parliament and the Council of the European Union, 'Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union', Brussels, (2016).
[253] European Commission, 'Revised Directive on Security of Network and Information Systems (NIS2)', Brussels, 2020.
[254] The European Parliament and the Council of the European Union, 'Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union', Brussels, (2016), Art. 6.
[255] Ibidem, Art.1.

the Member States whose, disjointed cybersecurity measures deter the protection of consumers and businesses, lowering "*the overall level of security of network and information systems*"[256].

As observed *inter alia* by Lohmann, the growing economic and political interdependence characterizing the 21st century has made economic diplomacy a preferred policy option in tackling national security threats[257]. Not surprisingly, core cybersecurity issues have been inextricably tied to the functioning of the internal market. Rules managing network and information security are drawn on personal data protection, e-commerce and electronic communications, which are areas linked to the internal market.

To further strengthen cybersecurity, the General Data Protection Regulation (GDPR)[258] came into force in the same year with the aim to safeguard EU citizens' personal data, by defining the regulatory environment.

The two ransomware attacks in 2017 under the names of *WannaCry* and *Petya* have evolved the understanding of cyber security, highlighting a number of key issues. First, cyber threats are the new reality of today's world, with unpredictable cascading and crippling effects, turning into a first business priority. Second, combating cyber-attacks necessitates strong collaboration across well-established networks made up of both public and private actors. Lastly, ineffective cybersecurity measures may hinder the efficient operation of the Digital Single Market (DSM) strategy[259], resulting in financial consequences for individuals, enterprises, and governments. Introduced in May 2015, the DSM strategy aspires for a universal digital economic zone, building on three main pillars: (*i*) improving access to digital goods and services, (*ii*) an environment where digital networks and services can prosper, (*iii*) digital as a driver for growth.

Furthermore, all these acknowledgements are reflected in the 2017 Joint Communication on *Resilience, Deterrence and Defence: Building Strong cybersecurity for the EU* , which indeed shows how the EU's understanding of the cybersecurity world has evolved, stressing the need for (*i*) greater resilience to cyber-attacks, (*ii*) detection of cyber-attacks, and (*iii*) international cooperation on cybersecurity.

Given all the above, enhancing cyber defence capabilities and expertise is instrumental for EU cyber-security. In this regard, the Commission has launched a slew of new initiatives, among which the

[256] Ibidem.
[257] Stanzel V. and others, 'New Realities in Foreign Affairs: Diplomacy in the 21st Century', (*SWP*, 2018), 11, pp. 12-17.
[258] European Parliament and the Council, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on 62 the free movement of such data, and repealing Directive 95/46/EC, (General Data Protection Regulation), Brussels, (2016).
[259] European Commission, 'Communication: A Digital Single Market Strategy for Europe', Brussels, (2015).

revision of the *Cyber Defence Policy Framework* (CDPF)[260], incorporating cybersecurity and cyber defence into a broader security and defence agenda titled *Military Vision and Strategy on Cyberspace as a Domain of Operation,* aiming to improve synergies, cooperation and interoperability in the defence areas.

Worth mentioning is also one of the most powerful diplomatic instruments, the *Cyber Diplomacy Toolbox,* to further strengthen EU international security and diplomacy. Adopted in 2017 by the EU Foreign Affairs Council, it underscores the essential principles for a joint diplomatic and appropriate response to hostile cyber activity, facilitating cooperation and promoting risk reduction planning. Along with a number of preventive, stabilizing and cooperative initiatives, it also includes a game-changer: a new Cyber Sanctions Regime (EUISS)[261], which has already been used to prosecute Chinese, Russian and North Korean nationals who were alleged responsible for Cloud Hopper, NotPetya and WannaCry, respectively[262].

A further update of the EU cybersecurity strategy came in December 2020, after a surge in cyberattacks exploiting uncertainty, fear and increasing vulnerabilities deriving from the COVID-19 pandemic[263]. The latter has sped up digitization and technologies at an unprecedented rate across numerous sectors, increasing exposure to cyber-attacks and other unwanted online activities. 2019 alone has registered 450 cybersecurity incidents targeting finance and energy companies, amounting to 10 billion euros paid out for ransomware attacks[264].

Notably, in 2019 President Ursula von der Leyen claimed that "*cyber security and digitalization are two sides of the same coin. This is why cybersecurity is a top priority*"[265].

The newly revised EU Cybersecurity Strategy[266] has been designed to address growing security threats by strengthening cyber threat resilience and awareness through detailed proposals for investment, regulatory and policy measures. The strategy lies on three main pillars: first, technological sovereignty and leadership across the community, further strengthened by the *Directive on measures for a high common level of cybersecurity across the Union* (NIS2)[267] and the *Directive*

[260] General Secretariat of the Council, 'EU Cyber Defence Policy', 14413/18, Brussels, (2018).
[261] The Council of the European Union, 'Council Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States', Brussels, (2019).
[262] Erskine S., 'The EU Tiptoes into Cyber Sanctions Regimes', (*RUSI*, 2020).
[263] Interpol, 'Cybercrime: Covid-19 Impact', (2020), pp. 4-6.
[264] Jovanovic B., 'A Not-So-Common Cold: Malware Statistics In 2022', (*Dataprot*, 2022), Available at: <https://dataprot.net/statistics/malware-statistics/>, (accessed 20 May 2022).
[265] Ursula von der Leyen, 'Speech in The European Parliament Plenary Session' (*European Commission* 2019), Available at: < https://ec.europa.eu/info/sites/default/files/president-elect-speech-original_1.pdf>, (accessed 20 May 2022).
[266] The European Parliament and the Council, 'Joint Communication: the EU's Cybersecurity Strategy for the Digital Decade', Brussels, (2020).
[267] The European Parliament and the Council, 'Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148', Brussels, (2020).

on the Resilience of Critical Entities (CER)[268]. Likewise, the promotion of a *European Cyber Shield* - aimed at building effective early warning systems and emergency plans - and the recent establishment of a *Joint Cyber Unit* (JCU) – intended to enhance IT defence capabilities and law enforcement cooperation - have boosted the information level exchange between the various stakeholders, allowing for effective incident detection and warning. Second, operation capacity represents a focal point in the prevention, detection, and response of cyber incidents. Finally, the third dimension is focused on the need for increased cooperation and consolidation, through which promoting European values. Coordination on cyber-related issues encompasses the involvement and interdependence between the national, European and global levels[269].

Overall, the current framework is closely linked to other Union measures, such as the EU Cybersecurity Act (2019)[270], the Commission's Economic Recovery Plan[271], and the Security Union Strategy 2020–2025[272].

2.2.1. The EU Cybersecurity Act

Business actors, including large, small and medium enterprises (SMEs), have progressively switched to cyberspace in their commercial activities, developing a modern e-commerce trading system. In Europe, e-commerce sales have registered the amount of 161 billion euros in 2019, growing to 717 billion in 2020[273]. The widespread application of connected devices across industries has posed substantial threats to multiple companies that, however, have continued to underestimate the cyber risk they are increasingly exposed to, translating into low investment and inadequate legal risk management[274].

---

[268] The European Parliament and the Council, 'Proposal for a Directive on the resilience of critical entities', Brussels, (2020).

[269] Kaspter A. and Mölder H., 'The EU's Common Security and Defence Policy in Facing New Security Challenges and Its Impact on Cyber Defence' in Ramiro Troitino D. and others, *The EU In The 21St Century* (Springer, 2020), pp. 271-288.

[270] The European Parliament and the Council of the European union, 'Regulation (EU) 2019/881 of the European Parliament and of the Council of 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', Brussels, (2019).

[271] The Council of the European Union, 'Council Regulation (EU) 2020/2094 of 14 December 2020 establishing a European Union Recovery Instrument to support the recovery in the aftermath of the COVID-19 crisis', Brussels, (2020).

[272] 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 on the EU Security Union Strategy', Brussels, (2020).

[273] 'Ecommerce In Europe: €717 Billion In 2020' (*Ecommerce News*, 2020), Available at: <https://ecommercenews.eu/ecommerce-in-europe-e717-billion-in-2020/>, (accessed 23 May 2022).

[274] European Commission, 'Commission Staff Working Document, Impact assessment accompanying the document proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification', (2017), p. 38-45.

Acknowledging this backdrop, the European Parliament has taken immediate steps towards a new Cybersecurity Act[275] (Regulation (EU) 2019/881), definitely entered into force in June 2019 within the framework of the Digital Single Market strategy, directed at strengthening the level of cybersecurity within the EU internal market.

Acting on the legal basis provided for by Art. 114 of the TFEU[276], the Cybersecurity Act arises from the EU's ambition of being a global leader in the cybersecurity industry, as well as from the awareness of the inadequacy of the existing regulatory framework, as evidenced by recent events.[277]

In this frame, the Act establishes a permanent EU body addressing cybersecurity threats and creates a pan-European Cybersecurity Certification Framework, defining compliance standards and procedures for businesses operating in EU countries while minimizing the costs of market fragmentation. Acting as business law, the Act advocates for the implementation of common certification standards for ICT goods, services, and processes, setting up evaluation criteria and a minimum level of cybersecurity assurance. To this purpose, a supervisory authority is nationally appointed to manage certification issuance, conformity and non-compliance penalties. Three main levels of assurance are specified in article 52[278]: basic, substantial and high, whose assessment depends on the level of incident risk. Although cybersecurity certifications are voluntary schemes, unless domestic laws provide otherwise, the Act provides minimum and mandatory requirements to align with.

Yet, because many have raised concerns over the lack of an explicit reference to IoT's technical security standards contributing to information asymmetries, the Commission has moved forward with new proposals to include the existing information security framework[279].

The passing of the Cyber Act has introduced several stakeholders to the scene. One of the main actors is the European Union Agency for Cybersecurity (ENISA)[280], which has been further strengthened by the EU cybersecurity Act with more resources and new goals, aiming for a higher level of cybersecurity and trustworthiness across the EU.

---

[275] The European Parliament and the Council of the European union, 'Regulation (EU) 2019/881 of the European Parliament and of the Council of 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', Brussels, (2019).

[276] European Union, 'Consolidated version of the Treaty on the Functioning of the European Union', 2009, Chap.3, Art. 114.

[277] Fantin S. 'Weighting the EU Cybersecurity Act: Progress or Missed Opportunity? ', (*CiTiP, KU Leuven Centre for IT & IP Law*, 2019), Available at: < https://www.law.kuleuven.be/citip/blog/weighting-the-eu-cybersecurity-act-progress-or-missed-opportunity/ >, (accessed 23 May 2022).

[278] The Council of the European Union, 'Council Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States', Brussels, (2019), Art. 52.

[279] European Commission, 'Rolling Plan for ICT Standardisation 2021', Brussels, (2021).

[280] The abbreviation ENISA comes from its original name, the European Network and Information Security Agency.

Since it was first launched in 2004, ENISA was entrusted with the task of providing advice and technical expertise to private stakeholders, Member states and EU offices in implementing and understanding the Directive on the Security on Network and Information System, raising cybersecurity standards and boosting infrastructures resilience. Besides carrying out consultancy activities with the support of ad-hoc expert groups, the agency has been recently conferred operational tasks, coordinating and harmonizing cybersecurity policies. As specified in Art. 6 of the Cybersecurity Act, ENISA will assist "*Member States in their efforts to improve the prevention, detection and analysis of, and the capability to respond to cyber threats and incidents by providing them with knowledge and expertise*"[281] and "*in developing national Computer Security and Incident Response Teams (CSIRTs), where requested*"[282]

Additionally, a newly formed Stakeholder Cybersecurity Certification Group (SCCG) has been launched to support both ENISA and the European Commission in smoothing strategic consultancy on cybersecurity certification and in drafting the Union Rolling Work Programme (URWP) – an annual paper identifying priorities for future cybersecurity certification schemes.

The ultimate objective of this intertwined structure is to strengthen cooperation between the Member States and the various EU stakeholders operating in cyber security landscape, including the private sector, in particular the providers of essential services mentioned in Annex II[283] of the NIS Directive and the providers of digital services mentioned in Annex III[284]. This poses evident problems when obligations are extended to the private sector. While the Member States are allowed to define criteria for penalties in case of infringement[285], indeed, this doesn't provide the private sector with any incentives to cooperate at its own commercial expenses, not it guarantees that the obligations established by regulations will not hinder innovation.

This cooperative approach has been adopted since cyberspace has completely destroyed all territorial borders, undermining the feasibility of existing national laws. As critical infrastructures - namely hospitals, railways, and utility networks just to name a few - are generally located within a country's territory, falling within its territorial justification, MS governments can preserve the status quo without referring to international law, avoiding the risks of fragmented jurisdictions[286]. This is

[281] The Council of the European Union, 'Council Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States', Brussels, (2019), Art. 6(a).
[282] Ibidem, Art. 6(d).
[283] The European Parliament and the Council of the European Union, 'Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union', Brussels, (2016), Annex II.
[284] Ibidem, Annex III.
[285] The European Parliament and the Council of the European Union, 'Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC', Brussels, (2016), Art.58.
[286] Fidler D. 'Wither the Web? International Law, Cybersecurity and Critical Infrastructure Protection', (*Georgetown Journal of International Affairs*, 2015), 8, pp. 8–20.

evidently clear in article 58 of the present Act, stipulating that "*each Member State shall designate one or more national cybersecurity certification authorities in its territory or, with the agreement of another Member State, shall designate one or more national cybersecurity certification authorities established in that other Member State to be responsible for the supervisory tasks in the designating Member State*"[287]. Yet, it remains rather uncertain how EU Member States will understand a "*cyber incident with a significant disruptive impact*"[288] and how they will guarantee the operators to notify such incidents to the appropriate authority.

Given the above, the State sovereignty principle is commonly agreed to apply in cyberspace, without being possibly claimed over the entire cyber landscape[289]. Once again, the argument lies in the different sovereign territories where cyber infrastructures are stationed, besides the fact that, in international legislation, territoriality allocates jurisdictional powers.

2.2.2. Limits and challenges of the European cybersecurity strategy

Technological progress has gone along with new cyber threats, bolstering EU defence capabilities with the need to protect European values and interests. Although impressive efforts have been made so far, raising challenges hampering the EU's ambition to achieve a greater level of security[290].

The 2013 Strategy refers to cybersecurity as "*the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure*"[291], whose primary objective results, hence, in the preservation of the integrity and availability of critical networks.

This interpretation differs from the contextual definition offered by ENISA, which allows stakeholders and policymakers, including EU agencies, to select the definition that is more suitable for their specific contextual needs[292]. Among the most common definitions, there are those provided by the *European Committee for Electrotechnical Standardization* (CENELEC), *the International*

[287] The Council of the European Union, 'Council Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States', (2019), Art.58.
[288] The European Parliament and the Council of the European Union, 'Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union', (2016), Art. 6.
[289] Sandage J. et al., 'Comprehensive Study on Cybercrime', (United Nations Office on Drugs and Crime, 2013), pp.183-184, Available at: <https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>, (accessed 27 May 2022).
[290] Mortera-Martinez C. 'Game over? Europe's cyber problem', (*Centre for European Reform,* 2018), pp. 5-7.
[291] European Commission and HREU, 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', (2013).
[292] ENISA, 'Definition of cybersecurity: gaps and overlaps in standardization', (2016), pp. 10-12.

Telecommunication Union (ITU) and *the International Organization for Standardization* (ISO), all emphasising different angles of cybersecurity, notably military, policy, economic or technical.
This flexibility raises significant risks when the conceptualization of the term is dangerously limited in its scope. Excessive inclusiveness or broadness of the term can obstruct the development of a coherent regulatory framework in the area, potentially causing frictions between EU institutions and Member States.
This ambiguity is likewise present in multiple legal measures on cybersecurity - mostly in the form of directives - which allow Member States to freely choose the methods and forms to implement the content. Fragmentation and gaps in the balance of responsibilities, along with transposition issues, risk growing in the long run as the cyber landscape evolves[293].
One of the major difficulties of cybersecurity regulations is identifying "*the right obligations to impose on the rights actors, through the right instruments*"[294] . Indeed, as outlined by Porcedda, there are "*at least eleven instruments of EU law having a bearing on [data and information security] breaches, five in the Area of Freedom, Security and Justice (AFSJ) and six in the internal market*"[295] . The pressing issue of identifying the right actors specifically surrounds the debate around the current EU Product Liability Directive 85/374/EEC[296], which indeed tends to facilitate some software developers.

Although there is no explicit reference to software as a product, some scholars have suggested including it within the category [297]. As established in Article 3 of the present directive, liability can be linked to anyone in the supply chain who, in turn, can be eventually demanded to compensate victims for "*any damage caused to the physical well-being or property, independently whether or not there is negligence on the part of the producer*"[298]. In other words, the EU has established a strict regime where there is no need of providing negligence proof against the individual or entity, but rather the causality between the damage and the defect. Yet, as specified, the regime cannot be

[293] European Court of Auditors, 'Challenges to effective EU cybersecurity policy', (2019), pp. 33-39, Available at: <https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf>, (accessed 27 May 2022).
[294] González Fuster G. and Jasmontaite L., 'Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights', In Christen M, Gordijn B, and Loi M, *The Ethics Of Cybersecurity* (Springer, 2020), pp.109.
[295] Porcedda M.G., 'Patching the patchwork: appraising the EU regulatory framework on cyber security breaches', (Computer Law and Security Review, 2018), 34(5), pp. 4.
[296] Council**,** 'Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products', (1985).
[297] Alheit K., 'The applicability of the EU product liability directive to software', (*Comparative and International Law Journal of Southern Africa*, 2001), pp. 188–209; Navas, S., 'Robot Machines and Civil Liability' in Ebers M., and Navas S., *Algorithms and Law*, (Cambridge University Press, 2020), 157-173.
[298] Council, 'Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products'**,** (1985), Art. 3.

invoked whenever the product causes economic damage or violates an individual's rights, as the damage should target a person or private property.

The lack of comprehensive protection of individual's security has led to numerous suggestions, among which, Daley's idea of balance, is the one thought to be helpful to the EC goal of "*high quality, affordable and trustworthy cybersecurity products*"[299]. In particular, Daley's approach focuses on a balance between ex-ante incentives to invest in security and ex-post liability, stressing trust and confidence in computer systems[300].

Although the efforts to increase coherence and coordination, the EU's approach to cybersecurity is still perceived as highly fragmented, with a "*lack of clearly delineated areas of responsibility and accountability among the different institutions*"[301].

At national level, coherence problems are evidently more acute. While some countries – notably France, the Netherlands, Italy and Germany – are more inclined to further develop the existing EU cybersecurity framework, some others – the Visegrad group[302] plus Austria, push for enhancing sub-regional cooperation. Priority discrepancies lie both in political options and in security potentialities, which include above all the implementation of an effective institutional framework where to share information with foreign countries and the ability to carry out cyber operations.

The coexistence of different national cybersecurity coordination models impedes a common agreement on a unique method for collecting and sharing information[303]. This results in the unwillingness of Member States to fund necessary infrastructure investment, overshadowing cybersecurity issues and thus, undermining the overall degree of protection of businesses and consumers. These divergencies are furtherly amplified by the lack of intersectoral cooperation, low levels of cybersecurity maturity, and diverging national and corporate interests balancing profit and security[304].

While the financial industry is widely more willing to cooperate, more hesitation is shown by telecommunication sectors and operators which fear an erosion of their competitive advantage[305].

---

[299] Vice-President Ansip, 'The Chatham house annual cyber conference: evolving norms, improving harmonisation and building resilience. Speech by Vice-President Ansip', (2017).

[300] Daley J., 'Insecure software is eating the world: promoting cybersecurity in an age of ubiquitous software-embedded systems', (*Stanford Technology Law Review*, 2016), 19(3), pp.538.

[301] Bendiek, A., 'European Cyber Security Policy', (SWP 2012), 13, pp. 20.

[302] It includes the Czech Republic, Hungary, Poland, and Slovakia.

[303] Christou, G. *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy*, (New Security Challenges Series 2016), pp.46.

[304] European Commission, 'Digital Economy and Society Index – DESI', (2021), pp. 15, available at: < https://digital-strategy.ec.europa.eu/en/policies/desi>, (accessed 28 May 2022).

[305] Carrapico H. and Barrinha A., 'The EU as a Coherent (Cyber)Security Actor? ', *(Journal of Common Market Studies*, 2017), 55(6), pp.1259-1261.

Once again, what causes major trouble is the legal attribution problem which threatens the effectiveness of cybersecurity rules and the implementation of its sanction regime[306]. The main reason lies in technical and legal difficulties which make the individualization of responsible actors exponentially difficult[307]. One of the main requirements to issue sanctions and restrictive measures is the capability to prove any maliciousness behind a cyber-attack, furtherly complicated by the decentralised nature of the cyber and information domain, the disparities across Member States and the absence of analytical capabilities at EU level. As a consequence, Member States tend to act (rather, react) autonomously, hindering the chances of a coordinated response at the EU level[308].

National divergencies in approaching foreign and deference matters have limited the organisational capacity of the Union, raising challenges and dilemmas on the EU's ambitions of Guardian of the cyberspace[309].

2.2.2.1. Privacy and Cybersecurity

As previously highlighted, privacy and security have become two major concerns of today's society, which has become increasingly reliant on the exchange of personal information and, thus, requiring options and rules governing and securing the transition and use of data. Specifically, the threat of unintended interferences revealing personal and intimate information poses new dangers to both our privacy and security. The first attempt to regulate data protection came from Germany's right to informational self-determination, in 1982, progressively inspiring other countries[310].

Numerous regulatory measures have been adopted so far to strengthen the security of businesses, citizens and public administration in the specific areas of digital communications and computer crime. The 1995 *Data Protection Directive* (95/46/EC)[311] have driven toward the harmonization of national data protection laws, where, however, the main principles have been challenged by the increasing process of data to fight crime. The free cross-border flows of data across private companies have unveiled national discrepancies on data protection, pushing towards further harmonization. This logic has progressively included data protection as a fundamental right in both Article 16 of the Treaty on

[306] Healey J., 'Beyond Attribution: Seeking National Responsibility for Cyberattacks', (*Atlantic Council*, 2012), pp. 5-7.
[307] Bendiek A. and Schulze M., 'Attribution: A Major Challenge for EU Cyber Sanctions an Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW' (*SWP*, 2021), 11, pp.7-9.
[308] Ibidem.
[309] Constant P., 'Guardian of the Galaxy? Assessing the European Union's International Actorness in Cyberspace', (College of Europe, 2021), pp.30-32.
[310] 'Decision of the Federal Constitutional Court of Germany as from 15 December 1983', (1983), Az 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83, BVerfGE 65, 1, Volkszählung.
[311] The European Parliament and the Council of the European Union, 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data', Brussels, (1995).

the Functioning of the European Union (TFEU) and Article 8 of the Charter of Fundamental Rights, which however have led to conflictual normative understandings of data uses. Whereas, a security approach concentrated on the preciousness of data processing, i.e. "*the use that internal security agencies can make of personal data in the interest of security*"[312], thus resulting mostly concerned with citizen's safety rather than with their individual rights.

With the adoption of the Lisbon Treaty, the two distinct logics were finally abandoned, and all different understandings and uses of data protection laws were erased, shaping efforts towards a higher degree of harmonization[313].

Although perceived as one of the most significant EU legislative efforts, the *General Data Protection* Regulation (2016/679) has raised numerous controversies among Member States, showing once again States' reluctancy to further coordination. Mainly, profound normative cleavages and trust gaps remain among national authorities.

Currently, the EU regime of data protection is focused on the idea of consent and control, allowing users to choose which and with whom to share information[314]. Accordingly, individuals are free to determine how much privacy to share on social media platforms, notably Facebook, Instagram, Google and other firms, that are, thus, supposed to respect consumers' interests. Many Internet services, however, enjoy monopolistic powers which tend to persuade users to accept any terms to join the online community, turning the self-responsibility principle into a harmful tool. The principle of self-determination (on which the data protection regime is currently based on), should thus switch to regulations on the processing of data[315].

Likewise, data protection involves the principle of data quality, data parsimony and purpose specification, deriving from both ethical assumptions and international customary law[316].

While the concept of privacy is closely related to data protection, and thus to data security, cybersecurity encompasses broader concerns that are not exclusively related to personal data. Among its key principles, notably confidentiality, integrity and availability, data protection falls within two

[312] Ripoll Servent A. 'Protecting or Processing? Recasting EU Data Protection Norms', in Wolf J. Schünemann and Max-Otto Baumann, *Privacy, Data Protection and Cybersecurity in Europe* (Springer 2017), pp.115.

[313] European Commission, 'Proposal for a directive of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM/2012/010 final', (2012,a).

[314] Cate, F. H., and Mayer-Schonberger, V., 'Tomorrow's privacy. Notice and consent in a world of Big Data', (*International Data Privacy Law*, 2013), 3(2), pp. 67–73.

[315] Schermer, B. W., Custers, B., and Van Der Hof, S., 'The crisis of consent: How stronger legal protection may lead to weaker consent in data protection', (*Ethics and Information Technology*, 2014), 2, pp. 171–182.

[316] Baumann M-O. and Schünemann W., 'Introduction: Privacy, Data Protection and Cybersecurity in Europe', in Schünemann W. and Baumann M-O., *Privacy, Data Protection and Cybersecurity in Europe* (Springer 2017), pp.1-3.

of the three objectives: the confidentiality of information processed in cyberspace and the integrity of computer systems.

Enshrined in the Universal Declaration of Human Rights[317] and the European Convention on Human Rights[318], the fundamental privacy right is traditionally addressed to "*protect individuals against intrusive surveillance from the state*"[319], and recently, from the corporate sector, as personal data is increasingly generating economic value.

All in all, the use of information and communication technologies (ICT) across multiple sectors of the economy has made information extremely valuable. Although ICT minimizes costs and boosts efficiency by offering 24-hour customer service and information, it raises questions in terms of availability. The constant availability of information makes them regularly vulnerable to attacks. Businesses are thus required to cope with this emerging trade-off between securing information and guaranteeing availability.

Besides the legal and financial aspects of cybersecurity threats, there is a growing number of ethical issues ranging from privacy, protection of data, accessibility, data integrity to transparency and accountability which reflects most of the debates within the EU[320].

Since the cybersecurity law was proposed, a few concerns on individual rights have been raised both by experts, human rights organizations and public electronic communications providers. The reason lies behind the high discretion and autonomy provided to Member States in the adoption of national regulatory frameworks aiming to ensure a higher level of information security. A stunning example is the Lithuanian Cybersecurity Law, which has ever since, suffered from a lack of transparency and engagement of the broader society, besides containing a number of highly controversial provisions[321]. Furthermore, due to the Snowden revelations which have highlighted the divergencies between U.S. and EU data privacy law, there has been a wide acknowledgement at the EU level that "*cyber security can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and EU core values*"[322].

---

[317] UN General Assembly, 'Universal Declaration of Human Rights', New York, (1948), 217 A (III).

[318] Council of Europe, 'European Convention for the Protection of Human Rights and Fundamental Freedoms', as amended by Protocols Nos. 11 and 14, Rome (1950), ETS 55, entry into force 3 September 1953.

[319] Wolf J. Schünemann and Max-Otto Baumann, *Privacy, Data Protection and Cybersecurity in Europe*, (Springer 2017), pp.4.

[320] Eriksson J. and Giacomello G., 'The Information Revolution, Security, And International Relations: (IR)Relevant Theory?', (*International Political Science Review*, 2006), 27, pp. 221–244.

[321] Jasmontaite L., and Pavel Burloiu V., 'Lithuania and Romania to Introduce Cybersecurity Laws', in Wolf J. Schünemann and Max-Otto Baumann, *Privacy, Data Protection and Cybersecurity in Europe*, (Springer 2017), pp. 131-139.

[322] European Commission and HREU, 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', Brussels, (2013), pp 4.

Although the EU cybersecurity strategy clash with numerous fundamental rights, notably equality, freedom of expression and freedom to conduct a business, legislative proposals tend to be narrowly focused on private and family life rights, along with the protection of personal data, ignoring the benefits of a holistic approach.

Overall, the debate around the trade-off between security and privacy remains with unanswered questions.

Chapter 3

Legal overview of the international bio-defence regime

3.1. Essential pillars of international biosecurity governance

The conservation of biological diversity has required effective biosecurity frameworks, addressing the aggressive spread of invasive species and the outbreaks of infectious diseases, whether naturally developed or deliberately caused. Compounding to the global biological threat landscape has been the increasing possibility of rogue states and terrorists exploiting biological agents as war weapons, with potential adverse health and environmental risks[323]. Recent globalization trends and technological advances have significantly exacerbated the threat spectrum, boosting progressively regional and international partnerships, and global instruments for non-proliferation and public health, aiming at improving awareness of modern practices and biosafety concerns[324].

International efforts have led to four main regulatory sources, all providing the legal backbone of the current global biosecurity regime: the Convention on Biological Diversity[325] (CBD), promoting and ensuring the conservation of biological diversity, the WHO's *International Health Regulations 2005*[326] (IHR), focusing on naturally occurring infectious diseases – with only a few aspects on deliberate and accidental releases; the *Biological and Toxin Weapons Convention*[327] (BTWC), defining legally binding non-proliferation measures to restraint the dangerous effects of deliberate disease outbreaks. To further empower conventional instruments, the UN Security Council unanimously voted for the adoption of Resolution 1540[328], addressing the risks of WMD proliferation to non-state actors.

The outbreak of coronavirus has further drawn attention to the devastating consequences of virulent infectious diseases and global health threats. Originating in Wuhan in late 2019, it soon turned into a global health emergency of international concern, questioning whether the existing mechanisms to prevent, control and respond to major infectious disease outbreaks constrain rather than ease rapid

[323] Walsh P.F., 'The Biosecurity Threat Environment', (*Intelligence, Biosecurity and Bioterrorism*, 2018), pp. 21–57.
[324] Sture J., Whitby S. and Perkins D., 'Biosafety, biosecurity and internationally mandated regulatory regimes: compliance mechanisms for education and global health security', (*Medicine, Conflict and Survival,* 2013), pp. 289-321.
[325] United Nations, 'Convention on Biological Diversity', Rio de Janeiro, (1992), Nairobi, 1992, entry into force 29 December 1993, 1760 UNTS 79, 31 ILM 818.
[326] World Health Organization, 'International Health Regulations', Geneva, (2005), 2509 UNTS 79, entry into force 15 June 2007.
[327] United Nations, 'Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects', Geneva (1980), 1342 UNTS 137, entry into force 2 December 1983.
[328] UN Security Council, 'Security Council resolution 1540', (2004), S/RES/1540.

action[329]. The 2019 Global Health Security Index analysis[330] unleashed the inadequacy of global health security capacities and capabilities, causing serious preparedness issues for future pandemic and epidemic threats[331]. Particularly, during COVID-19 inadequate IHR implementation and adherence by WHO's member states have been found[332], resulting in insufficient capacity to tackle the cascading impact of the pandemic crisis.

Experts' exhortation to strengthen international arrangements is boosting serious revaluations about international systems and mechanisms in place, emphasizing the need for a global health diplomacy based on a multidisciplinary and global approach[333].

3.1.1. The Convention on Biological Diversity (CBD) and the supplementary agreement Cartagena Protocol on Biosafety

The past 35 years have witnessed a biotech boom, most of it involving genetic engineering practices, definitely opening the doors to human enhancement. Since the mid-1980s, thousands of field experiments with genetically modified plants (GMPs) – also known transgenic plants – took place, rapidly reaching global markets and consumers[334]. Although they provide for more efficient use and development of genetic information, the rapidly expanding number of modern technologies have raised serious concerns about environmental and food safety[335]. This trade-off between expected benefits and additional risks has been subject to intense debates among regulators and scientists, who highlighted a growing gap between biotechnological developments and political responses[336]. Governments of developed nations were accused to respond inadequately to the perceived risks, exposing the public to unsafe conditions, while developing countries were claimed to lack the necessary scientific and regulatory capacities[337].

---

[329] Sohrabi C., 'World Health Organization declares global emergency: A review of the 2019 novel coronavirus' (COVID-19), (*International Journal of Surgery*, 2020), 76, pp. 71-72.
[330] Cameron E., Nuzzo J. and Bell. J., 'Global Health Security Index: Building Collective Action and Accountability', (*Center for Health Security*, 2019), pp.17-30, Available at: <https://www.ghsindex.org/wp-content/uploads/2019/10/2019-Global-Health-Security-Index.pdf>, (accessed 10 June 2022).
[331] Ibidem.
[332] Aavitsland P. and others, 'Functioning of the International Health Regulations during the COVID-19 pandemic', (*Lancet*, 2021), pp. 1283–1287.
[333] Vennis M.I. and others, 'Complementarity of International Instruments in the Field of Biosecurity', (*Policy and Practice Reviews*, 2022), pp. 6-7.
[334] Premanandh J., 'Global consensus –Need of the hour for genetically modified organisms (GMO) labeling', (*Journal of Commercial Biotechnology*, 2011), 17 (1), pp. 37–44.
[335] Jiang S., and others, 'Environment and food safety: a novel integrative review', (*Environmental Science and Pollution Research*, 2021), 28, pp. 11-16.
[336] Harris R.C., 'State Responses to Biotechnology: Legislative Action and Policymaking in the U.S., 1990–2010' , (*Politics and the Life Sciences*, 2015), 34(1), pp. 1-3.
[337] Falkner R., 'Regulating Biotech Trade: The Cartagena Protocol on Biosafety', (*International Affairs*, 2000), 76(2), pp.300.

International discussions for global biosafety standards finally led to the publication of the OECD[338] report *Recombinant DNA Safety Considerations*[339] in 1986. Later known as the Blue Book, it is the first biosafety document presenting scientific guidelines on the environmental, industrial and agricultural use of genetically modified organisms (GMOs), serving as a reference for the assessment and management of potential risks[340].

Since this first attempt toward an international biosafety network, the importance of developing a global convention for the conservation of biodiversity and the sustainable use of its components paved the way for comprehensive negotiations in the 90s[341].

Among the historical series of UN conferences and world summits throughout the 1990s, the so-called *Rio Earth Summit* or *Conference on Environment and Development* (UNCED) gathered political leaders, diplomats and scientists to debate environmental and development issues, boosting the conclusions of two important treaties: the *Convention on Biological Diversity* (CBD)[342] and the *UN Framework Convention on Climate Change*[343] (UNFCCC).

Originally designed to align the multiple agreements on the protection of wildlife, the CBD rapidly reached out beyond this initial narrow goal, finally introducing a comprehensive and holistic approach to the conservation of biological resources while building upon existing environmental agreements[344]- notably the *Convention on Wetlands of International Importance* (Ramsar)[345] and the *Convention on International Trade in Endangered Species* (CITES)[346]. With a record number of 165 signatories[347], the CBD finally entered into force in 1993, becoming the first global agreement on biological diversity.

---

[338] The Organization for Economic Co-operation and Development (OECD) serves as an international forum where governments share good practices, compare experiences and discuss new policies to improve their economic development and social well-being.

[339] Organization for Economic Co-operation and Development, 'Recombinant DNA Safety Considerations - Safety considerations for industrial, agricultural and environmental applications of organisms derived by recombinant DNA techniques', (1986), Available at: <https://bch.cbd.int/en/database/48487>, (accessed 4 June 2022).

[340] Schiemann J., 'The OECD Blue Book on Recombinant DNA Safety Considerations: it's influence on ISBR and EFSA activities', (*Environmental Biosafety Research*. 2006), pp. 1-3.

[341] McGraw M. D., 'The story of the Biodiversity Convention: From Negotiation to Implementation', in Le Prestre P.G., *Governing Global Biodiversity: the evolution and implementation of the Convention on Biological Diversity, (*Routledge, 2017), pp.12-15.

[342] United Nations, 'Convention on Biological Diversity', Rio de Janeiro, (1992), Nairobi, 1992, entry into force 29 December 1993, 1760 UNTS 79, 31 ILM 818.

[343] UN General Assembly, 'United Nations Framework Convention on Climate Change', New York, (1992), Rio de Janeiro, 1992, entry into force 21 March 1994, A/RES/48/189.

[344] Zedan H., 'The road to the biosafety protocol', in Le Prestre P.G., *Governing Global Biodiversity: the evolution and implementation of the Convention on Biological Diversity, (*Routledge, 2017), pp.16-25.

[345] United Nations Educational, Scientific and Cultural Organization, 'Convention on wetlands of international importance especially as waterfowl habitat', Ramsar, (1971), 996 UNTS 245, entry into force 21 December 1975.

[346] The World Conservation Union, 'Convention on International Trade in Endangered Species of Wild Fauna and Flora', Washington D.C., (1973), 993 UNTS 243, entry into force 1 July 1975.

[347] They now amount to 195 states.

The threefold objective of the CBC aims to (*i*) conserve biodiversity, (*ii*) promote sustainability and (*iii*) guarantee the equal sharing of benefits deriving from the use of genetic resources[348]. In other words, the Convention recognizes the need to protect both the environment and human health from the disruptive effects of modern technologies, although acknowledging the promising potential of biotech innovations in promoting human well-being. This twin aspect is evidently clear in Article 16(1) providing for "*the access to and transfer of technologies that are levant to the conservation and sustainable use of biological diversity*"[349] and in Articles 19(3) and 8, aiming to develop biotechnology safety procedures, with the overall goal of lowering major threats to biological diversity[350].

Unlike other multilateral negotiations on trade and security, one new feature about CBD is the concessions granted to developing countries over their national biological resources. As majority owners of the assets under negotiation, favourable concession agreements have been negotiated to developing nations, securing them access control on local genetic resources[351]. Thus, while responding to the southern development imperatives, the CBD seeks to coordinate the environmental exigencies of the North, which, in turn, would offer technological know-how, balancing the lack of experience and investments of biologically rich countries[352].

The tremendous revenue opportunities derived from the genetic species information have raised questions on who owns, who controls and who can profit from them, involving intellectual property rights, technology transfer, human health, financial resources and cultural issues[353].

Although there is no specific reference to human rights concepts, the CBD and its instruments have significantly contributed to shaping the normative relationship between the environment and human rights, becoming a reference for international human rights bodies[354]. The UN Special Rapporteur on Human Rights and the Environment have clearly outlined these developments, clarifying the role of the CBD in guaranteeing the protection and realization of human rights which, as specified, depends

[348] United Nations, 'Convention on Biological Diversity', Rio de Janeiro, (1992), Nairobi, 1992, entry into force 29 December 1993, 1760 UNTS 79, 31 ILM 818, Art.1.
[349] Ibidem, Art. 16.
[350] Biological diversity covers "*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*" (Art.2).
[351] McGraw D., '*The CBD*: *Key Characteristics and Implications for Implementation*', (*Reciel,* 2022),11(1), pp. 17-28.
[352] Tinker C., 'A "New Breed" of Treaty: The United Nations Convention on Biological Diversity', (*Pace Environmental Law Review*, 1995), 13(1), pp. 199-211.
[353]'The Convention on Biological Diversity', in Secretariat of the Convention on Biological Diversity, (*Global Biodiversity Outlook*, 2001), pp. 119-136, Available at: <https://www.cbd.int/gbo1/copyright.shtml>, (accessed 6 June 2022).
[354] Morgera, E., 'Dawn of a New Day? The Evolving Relationship between the Convention on Biological Diversity and International Human Rights Law', (*Wake Forest Law Review*, 2018), pp. 101-121.

on the successful prevention of biodiversity loss[355]. This acknowledgement narrows States' discretion in accomplishing the CBD objectives, imposing substantive and non-retrogressive obligations under human rights law[356]. These obligations favour the societal-public engagement and the efficient governance of socio-ecological systems[357], providing opportunities to enjoy environmental-related rights and equal access to justice and remedies[358].

Failure to comply with obligations to safeguarding and promoting the biodiversity of ecosystems has raised serious implications for human rights, as "*full enjoyment of human rights depends on a healthy and sustainable environment*"[359].

Although the Convention does not refer directly to the term 'framework', various authors consider it as a framework convention insofar it "*sets the tone, establishes certain principles and even enunciates certain commitments*"[360]. Being a legally binding instrument, the CBD offers flexible institutional guidelines and general objectives to be further defined in national laws and policies. While supporting national action on biodiversity within state jurisdictions, the CBD framework agreement provides a global structure promoting international cooperation[361]. This flexibility is highly appropriate for facing environmental challenges since biodiversity governance mechanisms are better customized to each State's economic and political setting[362].

However, this interactional approach faces multiple obstacles. First of all, the implementation of environmental policies at national level requires capacity factors that include scientific, technical and human resources, urging countries to "*establish and maintain programmes for scientific and technical education and training in measures for […] conservation and sustainable use of biodiversity*"[363].

---

[355] Knox, J.H., 'Report of the Special Rapporteur on the Issue of Human Rights Obligations Relating to the Enjoyment of a Safe, Clean, Healthy and Sustainable Environment', (*Knox Biodiversity Report*, 2017), pp. 4-6, Available at: < https://digitallibrary.un.org/record/861173#record-files-collapse-header>, (accessed 6 June 2022).
[356] Ibidem, p. 12.
[357]Rodríguez-Garavito C., 'A Human Right to a Healthy Environment? ', in Knox J. and Pejan R., *The Human Right to a Healthy Environment* (Cambridge University Press, 2018), pp. 155–68.
[358] E. Hey, 'The Interaction Between Human Rights and the Environment in the European Aarhus Space', in Grear A. and Kotzé L.J., *Research Handbook on Human Rights and the Environment* (Edward Elgar, 2015), pp. 353–376.
[359] Koh N.S., Ituarte-Lima C. and Hahn T., 'Mind the Compliance Gap: How Insights from International Human Rights Mechanisms Can Help to Implement the Convention on Biological Diversity', (*Transnational Environmental Law*, 2022), 11(1), pp. 41.
[360] Snape J. W., 'Joining the Convention on Biological Diversity: A Legal and Scientific Overview of Why the United States Must Wake Up ', (*Sustainable Development Law & Policy*, 2010), 10(3), pp.8; Sánchez V. and Juma C., *Biodiplomacy: Genetic Resources and International Relations*, (African Centre for Technology Studies, 1994), pp. 322.
[361] McGraw D., '*The CBD*: *Key Characteristics and Implications for Implementation*', (*Reciel*, 2022),11(1), pp. 17-28.
[362] Abbott K.W and Snidal D., 'Hard and Soft Law in International Governance', (*International Organization*, 2000), 54(3), pp. 421–56.
[363] United Nations, 'Convention on Biological Diversity', Rio de Janeiro, (1992), Nairobi, 1992, entry into force 29 December 1993, 1760 UNTS 79, 31 ILM 818, Art.12.

Although Parties have implemented some measures to improve their own capacity, limited progress has been made toward this target[364]. Despite external assistance and training activities, developing countries and transition economies are the ones mostly suffering from institutional inadequacy, along with little financial support and limited human resources[365]. Likewise, although developed countries benefit from multiple financial resources, they lack both economic instruments and incentive mechanisms for conservation initiatives[366].

Overall, institutional-related challenges are mostly associated with coordination difficulties among governmental bodies and poor allocation of roles and responsibilities between the central and subnational levels, which have also resulted in poor documentation status and inadequate assessment[367] - furtherly constrained by the lack of consensus on common biodiversity baselines. For instance, while in Malaysia relevant agencies have not been entrusted with implementation duties, which has caused a lack of accountability[368], in South Sudan, the division of responsibilities between national and state governments has reflected a lack of ownership[369].

Similarly, lack of knowledge and accessible information represents a major obstacle to CBD implementation efforts. Although Article 14 of the Convention sets public participation as a prerequisite "*for a more transparent process of environmental impact assessment of community owned natural resources*"[370], more than half of countries have reported an absence of public participation and awareness, along with a lack of effective partnerships and engagement of the scientific community, resulting in the inability to undertake adequate measures to conserve biodiversity[371]. This is specifically true for developing countries where the lack of appropriate technicalities hinders the preparedness for biological disturbances and beyond. Compounding to this issue is the fact that many have not yet assessed which techniques they would need from developed countries[372].

---

[364] Van Deveer S.D. and Dabelko G.D., 'It's Capacity, Stupid: International Assistance and National Implementation', (*Global Environmental Politics*, 2001), pp. 18–29.
[365] Rosendal G.K., *The Convention on Biological Diversity and Developing Countries*, (Springer, 2000), pp.67-89.
[366] Le Prestre P.G., 'The CBD at Ten: The Long Road to Effectiveness', (*Journal of International Wildlife Law and Policy*, 2002), 5(3), pp. 269–285.
[367] Chandra A. and Idrisova A., 'CBD: A Review of National Challenges and Opportunities for Implementation', (*Biodiversity and Conservation*, 2011), 20(14), pp. 295–316.
[368] Government of Malaysia, 'Fifth National Report to the CBD', (2014), p. 90, Available at: <https://www.cbd.int/doc/world/ my/my-nr-05-en.pdf>, (accessed 7 June 2022).
[369] Republic of South Sudan, 'Fifth National Report to the CBD', (2015), p. 27, Available at: <https://www.cbd.int/doc/world/ss/ss-nr-05-en.pdf>, (accessed 7 June 2022).
[370] United Nations, 'Convention on Biological Diversity', Rio de Janeiro, (1992), Nairobi, 1992, entry into force 29 December 1993, 1760 UNTS 79, 31 ILM 818, Art.14.
[371] UNEP, 'Implementation of the Convention and its Strategic Plan', (2016), Available at: <http://cbd.int/kb/record/decision/11020?RecordType=decision&Subject=STRAT>, (accessed 7 June 2022).
[372] Morato-Leite J.R. and others, 'Experience, Mistakes and Challenges: The Implementation of the Convention on Biological Diversity in Brazil' in Jeffery I.M, Firestone J. and Bubna-Litic L., *Biodiversity Conservation, Law and Livelihoods: Bridging the North-South Divide*, (Cambridge University Press, 2008), pp. 155-180.

A third challenge marked by national authorities refers both to the difficulties of sectoral policies to absorb environmental and biodiversity issues and inconsistencies in the application of relevant measures. In other words, specialized productive sectors poorly reflect biodiversity conservation targets. In India, the overlapping regulatory regimes on agriculture, fisheries, environment and forests have resulted in increasing vagueness around enforcement mechanisms and competition over the limited governmental resources available[373]. Whereas, in South Africa, the integration of biodiversity concerns into sectors is expected to take about 10 years, requiring a long-term commitment[374].

Overall, all these factors have slowed down the uptake of CBD guidelines into national policies, further affected by the lack of monitoring and compliance provisions, which have been defined as vague and confusing[375].

To enhance the level of biodiversity protection, in 1995, an Ad Hoc Working Group on Biosafety[376] was established to write a complementary draft protocol - subsequently known as the *Cartagena Protocol on Biosafety to the Convention on Biological Diversity*[377] – with a set of binding rules specifically addressing the "*transboundary movement of any living modified organism (LMOs) resulting from modern biotechnology that may have adverse effects on the conservation and sustainable use of biological diversity*"[378]. Entered into force in 2003, the dual-purpose Protocol aims to build an enabling environment where to apply safety biotechnologies, maximizing their potentiality while limiting possible risks. By imposing the implementation of specialized bureaucracies within the State Parties to identify and track the transborder movement of LMOs, the Protocol has significantly contributed to the development of domestic biotechnology regulatory systems reconciling environmental and trade objectives[379].

[373] Ministry of Environment, Forest and Climate Change, Government of India, 'Voluntary Peer-Review under the Convention on Biological Diversity. Case Study 2: India', Available at: <https://www.cbd.int/doc/nbsap/in-vpr-en.pdf>, , (accessed 7 June 2022).
[374] Republic of South Africa, 'Fifth National Report to the CBD', Mar. 2014, p. 80, Available at: <https://www.cbd.int/doc/world/za/za-nr-05-en.pdf>, (accessed 7 June 2022).
[375] Aggarwal-Khan S., *The Policy Process in International Environmental Governance*, (Palgrave Macmillan, 2011), pp.5.
[376] Made up of legal and technical experts, the Ad Hoc Group was entrusted of negotiating international instruments governing the use and conservation of biological diversity, securing sufficient flexibility to accommodate future technology trends.
[377] United Nations, 'Cartagena Protocol on Biosafety to the Convention on Biological Diversity', Montreal, (2000), 2226 UNTS 208, entry into force 11 September 2003.
[378] Ibidem, Preamble.
[379] Bail C. and Falkner R., *The Cartagena Protocol on Biosafety: Reconciling Trade in Biotechnology with Environment and Development*, (Routledge, 2001), pp. 457-467.

Developed by politicians and lawyers jointly, the Cartagena Protocol is claimed to be "*inherently not amenable to science*"[380]. Numerous articles relate to other annexes or articles, intertwining concepts and procedures that make its understanding even harder[381].

The major obstacle the Protocol faces is its conflictual relationship with the WTO system[382] which, in turn, contains rules that refer to the trade of GMOs. While the Protocol establishes the precautionary principle to manage potential risks– thus imposing the deferral of any action whose effects lack significant scientific evidence - WTO seeks to prevent any limitation to trade, thus demanding scientific justification for any trade-restrictive initiatives. Because GMOs lack scientific certainty, any action could result in a breach of WTO rules[383].

Following the general rules of treaty interpretation, it has been argued that the Protocol overturns the WTO system because of its specificity and recentness. However, the Protocol's language in relation to other international agreements is rather contradictory. Although no substantial provisions specifically address the issue, the Preamble affirms that the Protocol's implementation does not imply any change in the obligations and rights of a Party under existing international agreements, which, however, must not be translated into the Protocol subordination. Besides, the Protocol has included a rather ambiguous savings clause, recognizing that "*trade and environmental agreements should be mutually supportive with a view to achieving sustainable development*"[384]. Given its vagueness which has resulted in varying national interpretations, the relationship between the two systems is thus not clarified, and the question remains opened[385].

What leads numerous authors to believe the Cartagena Protocol is condemned to fail is its misleading foundation[386]. Scientific studies from both EU research centres and US Scientific Academies highlight no connection between LMOs and new and/or greater threats than those posed by conventional technologies. Despite the worldwide distribution, there is still no reported case of LMOs causing any

---

[380] Falkner R., 'Regulating biotech trade: the Cartagena Protocol on Biosafety', (*International Affairs*, 2000), 76(2), pp. 299-313.

[381] Segger M-C., Perron-Welch F. and Frison C., *Legal Aspects of Implementing the Cartagena Protocol on Biosafety*, (Cambridge University Press, 2013), pp. 205-208; Egziabher T., 'The Cartagena Protocol on Biosafety: History, Content and Implementation from a Developing Country Perspective', in Traavik T. and Ching L.L., *Biosafety First*, (Tapir Academic Press, 2007), pp. 389-390.

[382] At present, both the World Trade Organization (WTO) and the Cartagena Protocol regulate the trade of GMO. Yet, while the former wishes to expedite the movement of goods in a free trade area, the latter aims to foster a safer trade, while limiting it for ecological reasons.

[383] Kedgley L.A., 'Is it Better to Be Safe than Sorry? The Cartagena Protocol Versus the World Trade Organisation', (*Victoria University of Wellington Law Review*, 2005), 36(2) pp. 438.

[384] Cordonier Segger M.C., Perron-Welch F. and Frison C., *Legal Aspects of implementing the Cartagena Protocol on Biosafety*, (Cambridge, 2013), p.46.

[385] Kedgley L.A., 'Is it Better to Be Safe than Sorry? The Cartagena Protocol Versus the World Trade Organisation', (*Victoria University of Wellington Law Review*, 2005), 36(2) pp. 427-468.

[386] McHugan A., 'Problems with the Cartagena Protocol', (*Asia Biotechnology*, 2006), 10(12), pp. 684-685; Cosbey A., Burgiel S., 'The Cartagena Protocol on Biosafety: An analysis of results', (*International Institute for Sustainable Development*, 2000), pp. 15-17.

harm to biodiversity. Instead, the Protocol omits any reference to the possible benefits of GMOs, which leads people to believe that potential advantages outweigh any potential risks[387]. As stated in Article 26, when making decisions on imports, States might consider "*socio-economic considerations arising from the impact on LMOs on the conservation and sustainable use of biological diversity*"[388]. Yet. the little knowledge of the positive impacts of GMOs on the global food supply hinders States to take such aspects into account.

3.1.2. International Health Regulations (IHR [2005])

The spread of infectious diseases in the 90s cast some doubts on the International Health Regulations' (IHR) effectiveness in flexibly responding to emerging threats. The critiques addressed the narrow scope of the regulatory control – applying to a short list of infectious diseases, non-compliant behaviours- and the lack of responsive strategic planning to rapid changes in the public health global environment[389]. By 1995, the World Health Academy[390] (WHA) acknowledged the need to break with traditional approaches and define a modern health and security framework in an era of globalization[391]. The advent of Severe Acute Respiratory Syndrome (SARS) in 2003 hasten the IHR revision process, leading to a complete proposed text in 2003[392] serving as a basis for following consultations. Two years later, the Assembly adopted the revised version of IHR, shaping a new legal framework for responding to public health risks and emergencies favouring a dynamic and all-encompassing approach.

Within the framework of 66 articles and 9 annexes, the new IHR has added a number of structural and capacity-building obligations which boost its overall goal "*to prevent, protect against, control and provide a public health response to the international spread of disease*"[393], while balancing States' duty to secure their citizens' health with their obligations to implement health-protective measures that do not unnecessarily interfere with international movement and trade. Particularly, Parties are

[387] Deborah Katz, 'The Mismatch Between the Biosafety Protocol and the Precautionary Principle', (*Georgetown International Environmental Law Review*, 2000), 13, pp. 949-950.
[388] United Nations, 'Cartagena Protocol on Biosafety to the Convention on Biological Diversity', Montreal, (2000), 2226 UNTS 208, entry into force 11 September 2003, Art.26.
[389] Fidler P.D. and Gostin L., 'The New International Health Regulations: An Historic Development for International Law and Public Health', (*Maurer Faculty*, 2006), pp. 85-90.
[390] It is a non-governmental organization in the field of medicine, assisting nations and medical societies in tacking jointly health issues, articulating health standards and guidelines, sharing expertise, means and methods to improve the social welfare services worldwide.
[391] World Health Assembly, 'Revision and Updating of the International Health Regulations', Geneva, (1995), WHA48.7.
[392] World Health Assembly, 'Revision of the International Health Regulations', Geneva, (2003), WHA56.28.
[393] World Health Organization, 'International Health Regulations', Geneva, (2005), 2509 UNTS 79, entry into force 15 June 2007, Art.2.

required to develop and enhance their detection and notification capabilities – furtherly spelt out in Annex 1 - to respond promptly to health emergencies[394]. Minimum capacity requirements - drawn on the 2002 Progress Report on the revision of IHR - are to be set up at local, regional and national levels, with the goal of establishing a global minimum standard.

However, the novelty of the new IHR should not mask the obstacles surrounding it.

As explained above, national governments are called upon to establish surveillance systems for health security monitoring and detection[395]. Compounding to this issue is the lack of specific quantitative and qualitative guidelines on how to conduct surveillance[396]. This presents a challenge for developing countries since most of them argue the lack of adequate infrastructure means[397]. As the majority of global infectious diseases arise in developing nations where people have limited access to essential health services, ensuring appropriate safety infrastructures is highly important. National non-governmental organizations (NGOs) have actively assisted governments in strengthening surveillance capacities, the absence of specific expertise has, however, caused inaccurate analysis and reporting[398]. Middle-income nations, instead, have spontaneously strayed from the recommended measures because of their negative economic impact. Some have indeed claimed the IHR requirements benefit wealthy nations who can swiftly deploy their own resources and respond more promptly to a global health threat notified via IHR processes while they make poorer countries divert their limited public health resources from managing domestic public health threats[399].

Although the Regulation's flexibility approach provides national governments with a greater room for manoeuvre in adapting appropriate mechanisms to their own economic and political context, it simultaneously risks incentivizing inaccurate public health reporting systems[400].

What is mostly contested is the lack of legal authority to impose the existence of surveillance mechanisms or to specify quality requirements[401]. Indeed, compliance seems to be left to States'

[394] Ibidem, Art.5.
[395] World Health Organization, 'International Health Regulations', Geneva, (2005), 2509 UNTS 79, entry into force 15 June 2007, Art.6.
[396] Sturtevant J.L., Anema A. and Brownstein J.S., 'The new International Health Regulations: considerations for global public health surveillance', (*Disaster Medicine and Public Health Preparedness*, 2007), pp. 117-118.
[397] Gostin L.O., 'Pandemic influenza: public health preparedness for the next global health emergency', (*Law, Medicine and Ethics*, 2004), pp. 565–573.
[398] Sturtevant J.L., Anema A. and Brownstein J.S., 'The new International Health Regulations: considerations for global public health surveillance', (*Disaster Medicine and Public Health Preparedness*, 2007), pp.118-119.
[399] Wilson, K., Halabi, S. and Gostin, L.O, 'The International Health Regulations (2005), the threat of populism and the COVID-19 pandemic', (*Global Health*, 2020), pp. 1-4.
[400] Mandl K.D., Overhage J.M., 'Wagner M.M., and others, 'Implementing syndromic surveillance: a practical guide informed by the early experience', (*Journal of American Medical Informatics Association*, 2004), pp. 141–150.
[401] Katz R., and Fischer J., 'The Revised International Health Regulations: A Framework for Global Pandemic Response', (*Global Health Governance*, 2010), 3(2), pp.12-13; Kluge H. and others, 'Strengthening global health security by embedding the International Health Regulations requirements into national health system', (*BMJ Global Health*, 2018), pp. 4-5.

discretion, largely depending on their reporting abilities[402]. Hence, current systems of surveillance work on the government's transparency and engagement, which might be impacted in case of corruption and political instability. Some nations may not understand the real value that IHR compliance can bring, particularly when illness reporting has the potential to do significant economic harm. Meanwhile, inadequate reporting can hinder the government's capacity to map and respond quickly to real-time health threats[403].

To enhance compliance requirements, Article 54 IHR requires each State Party to submit annually mandatory reports to the WHA. The traditional model named *Monitoring Questionnaire* – consisting of more than 250 self-assessment questions on core capacities – was soon replaced in 2018 by the *State Party Self-Assessment Annual Reporting Tool* (SPAR), relying instead on 24 criteria for 13 of the IHR capabilities listed in Annex 1[404]. The launch of the new instrument was conceived to enhance States' compliance with reporting duties and related to reducing capacity gaps in the implementation of core requirements. Although the new approach has successfully contributed to the increased number of States submitting annual reports, some authors report the new model's lack of clarity in describing the core capacities, which contributes to the failure of Parties to implement the required measures[405].

That being said, what makes the monitoring system even more unstable is the lack of clarifications concerning States' obligations. Although national reports are made public, they are not subject to any review or follow-up, which reflects "*state party concern with maintaining sovereignty on politically sensitive matters*"[406]. Besides, incomplete or missing submissions are not followed by formal penalties. This self-assessment approach, together with the lack of compliance evaluation and accountability mechanisms, hinder the chances to improve indications of the thresholds States are required to fulfil. Thus, relying on a system largely based on self-assessments, it has been

[402] Gostin L.O., Katz R., 'The International Health Regulations: The Governing Framework for Global Health Security', (*Milbank Q*, 2016), pp. 276-279.
[403] Wilson, K., Halabi, S. and Gostin, L.O. 'The International Health Regulations (2005), the threat of populism and the COVID-19 pandemic', (*Global Health*, 2020), 16(70), pp. 2-3.
[404] WHO, 'IHR State Parties Self-Assessment Annual Reporting Tool', Available at: < https://apps.who.int/iris/bitstream/handle/10665/272432/WHO-WHE-CPI-2018.16-eng.pdf?sequence=>, (accessed 12 June 2022).
[405] Bartolini G., 'The Failure of Core Capacities under the WHO International Health Regulations', (*British Institute of International and Comparative Law*, 2021), pp. 234-241; Kay A. and Williams O., *Global Health Governance: Crisis, Institutions and Political Economy*, (Palgrave Macmillan, 2009), pp. 74-76.
[406] Taylor A. and Habibi R., 'The Collapse of Global Cooperation under the WHO International Health Regulations at the Outset of COVID-19: Sculpting the Future of Global Health Governance', (*American Society of international Law*, 2020), 24(15), pp. 5.

demonstrated that more than half of States Parties have registered low scores ranging from 1 to 3, with a poor or modest level of preparedness[407].

Finally, another downside is the lack of any provisions ensuring close and meaningful cooperation between states and the WHO itself. Although Article 44 outlines countries' obligation to collaborate and assist one another, it is merely confined to health issues, suggesting limited international solidarity[408]. This is further emphasised in article 2 explaining that "*the purpose and scope are to prevent the international spread of disease in ways that are […] restricted to public health risks*"[409]. IHR agreement should, however, be interpreted consistently with other relevant international treaties, as it seeks not to affect "*the rights and obligations of any State Party deriving from other international agreements*"[410]. Yet, problems arise in pandemic situations when States are required to deal with a wide range of conflicting provisions under different agreements[411].

Acknowledging the impact of public health interventions on political and civil rights, the revised agreement incorporates human rights principles, proclaiming that "[*t]he implementation of the Regulations shall be with full respect for the dignity, human rights and fundamental freedoms of persons*" and "*guided by the Charter of the United Nations and the Constitution of the WHO*"[412]. Although very broad, the provision in Art. 3(1) defines the link between the international human rights system and the Regulation itself, incorporating it within the legal framework of the 2005 IHR, consequently imposing a duty on States Parties to ensure the implementation of the Regulation's health measures compliant with human rights standards. Nevertheless, it serves more as a guideline rather than representing a binding provision [413], raising questions on how to interpret and implement it properly.

The outbreak of coronavirus disease 2019 has further unleashed the ineffective performance of IHR management and supervision[414], questioning its credibility as a legal and public health tool. The major

[407] WHO, 'Thematic Paper on the Status of Country Preparedness Capacities', (2019), Available at: <https://www.gpmb.org/annual-reports/overview/item/thematic-paper-on-the-status-of-country-preparedness-capacities>, (accessed 12 June 2022).
[408] Fidler D.P., 'From International Sanitary Conventions to Global Health Security: The New International Health Regulations' (Chinese Journal of International Law, 2005), 4(2), pp. 374-376.
[409] World Health Organization, 'International Health Regulations', Geneva, (2005), 2509 UNTS 79, entry into force 15 June 2007, Art.2.
[410] World Health Organization, 'International Health Regulations', Geneva, (2005), 2509 UNTS 79, entry into force 15 June 2007, Art.57(II).
[411] Lee J. 'IHR 2005 in the Coronavirus Pandemic: A Need for a New Instrument to Overcome Fragmentation? ', (*Asil insights*, 2000), 26(16).
[412] World Health Organization, 'International Health Regulations', Geneva, (2005), 2509 UNTS 79, entry into force 15 June 2007, Art. 3(I).
[413] Zidar A., 'WHO International Health Regulations and Human Rights: From Allusions to Inclusion', (*British Institute of International and Comparative Law*, 2015), pp.9-10.
[414] WHO, 'Strengthening preparedness for health emergencies: implementation of the International Health Regulations (2005), (2021), pp.4-5.

setback lies in the WHO's role, which is largely limited to collecting data, distributing information, and providing recommendations, thus failing its coordination role between governments and international organizations. It follows the states' discretion to interpret WHO guidelines, which results in disjointed, compartmentalized, and fragmented measures[415]. Taking the Covid-19 experience, some Asian countries have shown greater preparedness than others, because of their deliberate fortification of national regulatory systems[416]. This fragmentation is feared to compromise in the short run the global efforts to contain a public health crisis, highlighting the need for a systemic approach. Although the fractured nature of international law is explicitly recognized by the IHR 2005, it doesn't provide any guidelines to overcome it.

3.1.3. The Biological Weapons Convention (BWC)

Since ancient times, there has been an increasing interest and use of biological warfare agents, whose practice was officially condemned within the framework of the 1907 Hague Convention IV Respecting the Laws and Customs of War on Land[417]. Further efforts to reinforce this restriction resulted in the signing of the Geneva Protocol in 1925[418], which prohibited the use of both chemical and bacteriological warfare tactics. Of major concern was however the lack of a complete ban on the development, production and stockpiling of such weaponry. Many States signatories made indeed reservations declaring the cease of the Protocol's binding nature in case of non-fulfilment of the contract obligations by enemy states[419]. This legal flexibility allowed Governments to pursue BW research and arm race programmes[420].

The two World Wars advanced the need for world peace, leading in March 1975 to the ratification of the *Convention of the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction*[421].

---

[415] Spicer N., Agyepong I., Ottersen T., Jahn A., Ooms G., 'It's far too complicated': why fragmentation persists in global health', (*Global Health*, 2020), 16(1), pp. 2-20.
[416] Brian Y. and Shui-Yan T., 'From COVID-19 Responses in East Asia: Institutional Infrastructure and Enduring Policy Instruments', (*American Review of Public Administration*, 2020), pp. 791-794.
[417] International Peace Conferences, 'Hague Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land', The Hague, (1907), entry into force 26 January 1910.
[418] United Nations, 'Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or other Gases, and of Bacteriological Methods of Warfare', Geneva, (1925), entry into force 8 February 1928.
[419] Pilloud C., 'Reservations to the Geneva Conventions of 1949', (*International Review of the Red Cross*, 1976), pp. 107-109.
[420] Huigang L., and others, 'Development of and prospects for the biological weapons convention', (*Journal of Biosafety and Biosecurity*, 2022), 4(1), pp. 50-53.
[421] United Nations, 'Convention of the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction', Geneva, (1971), 1015 UNTS, entry into force 26 March 1975.

The BW Convention represented the first world's multilateral disarmament agreement which requires state parties "*never in any circumstances to develop, produce, stockpile or otherwise acquire or retain […] microbial or other biological agents, or toxins whatever their origin or method of production*"[422]. It follows the responsibility for State parties to implement the necessary measures to prevent and prohibit what stipulated in Article 1. The ban applies only to biological agents "*of types and in quantities that have no justification for prophylactic, protective or other peaceful purposes*"[423]. Should a signatory have any biological agents, it has nine months' time since the convention's entrance into force to destroy or redirect its stockpiles for peaceful purposes[424]. The BWC does not provide however any definition of the prohibited items, neither of what constitutes biological activities for 'peaceful purposes'. The lack of precise definitions further complicates the understanding and implementation of states' obligations, which might result in the production – whether in laboratories or in the field - or the acquisition of certain agents[425].

Equally relevant is the lack of restrictions on biological research activities[426]. This omission is linked to the difficulties of distinguishing defensive from offensive biological research, offering States an opportunity to evade the Convention's provisions and avoid its penalties. Indeed, the duty to provide justification for any development, production or stockpiling of biological agents is not sufficient: besides the lack of standard criteria on the accepted quantities of agents or toxins that a State can develop, Parties are not even required to notify the amount, purpose or type of agents they develop and what use they make of them. The material accountancy method – mostly applied to verify certain arms control agreements - is not suitable when treating biological or toxin agents. It is thus unclear how much of a forbidden substance would be considered a breach of the Convention. The intense secrecy that surrounds biological weapons programmes thus raises suspicions and leads to charges of violations[427].

A similar vagueness surrounds the prohibition of transfer of agents, toxins or weapons to "*any recipient whatsoever*"[428], meaning any State, international agency or sub-national government. It involves thus the ban on assisting, encouraging or inducing potential actors to acquire the prohibited substances[429]. These non-proliferation provisions contrast with the content of Article X, which

[422] Ibidem, Art.1.
[423] Ibidem.
[424] Ibidem, Art. 2.
[425] Goldblat J., 'The Biological Weapons Convention - An overview', (*International Review of the Red Cross*, 1997), pp.253.
[426] Ibidem, pp. 254.
[427] Trapp R., 'Compliance Management under the Chemical Weapons Convention', (*WMDCE*, 2019), pp. 8-12.
[428] United Nations, 'Convention of the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction', Geneva, (1971), 1015 UNTS, entry into force 26 March 1975, Art.3.
[429] Ibidem.

specifies the Parties' responsibility to undertake the exchange of biological agents' information or equipment for peaceful purposes. Although an informal forum of countries - named Australia Group (AG) - has harmonized export controls on any items' transfer to reduce misuse risks, many nations do not consider the Group's export restrictions as binding, declaring them discriminatory[430]. In other words, since the Convention was designed as a disarmament agreement, cooperation on technology development and application in biology looks rather difficult.

Furthermore, of major debate is its relationship with the 1925 Geneva Protocol. Although the BW Convention doesn't mention any prohibition to the use of biological or toxin weapons, it affirms the validity and bindingness of the Geneva Protocol's obligations, which in turn prohibit such use[431]. Yet, States who adhered to the BW Convention do not necessarily coincide with those who signed the Geneva Protocol. Moreover, what causes major trouble is the Convention's statement that "*nothing in its provisions shall be interpreted as in any way limiting or detracting from the obligations assumed by States under the Geneva Protocol*"[432], which results in the continuity of the Protocol's reservations. However, when the latter concern the right to employ biological weapons against non-contracting parties, they clash with the obligation of the parties to never "*in any circumstances acquire biological weapons*"[433].

When reservations regard the right to use the weapons against non-adherents of the Protocol or against a non-fulfilling Member State, there is an evident clash both with the Convention's obligation to never 'in any circumstances' acquire biological weapons and with the parties' willingness to exclude any possible use of biological agents as weapons of warfare[434].

In light of the above, it comes as no surprise the Iran's suggestion on the Convention's amendment, involving an explicit reference to the ban on us, which however did not receive wide support, mainly because of concerns that one amendment could trigger new negotiations[435].

No compliance mechanisms are offered to verify potential hostile intentions. As previously mentioned, parties are not required to notify the competent authority of non-prohibited activities involving biological agents or toxins. Nor are they compelled to inform of material research

[430] Goldblat J., 'The Biological Weapons Convention - An overview', (*International Review of the Red Cross*, 1997), p. 255.
[431] United Nations, 'Convention of the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction', Geneva, (1971), 1015 UNTS, entry into force 26 March 1975, Art.8.
[432] Ibidem.
[433] Ibidem, Art.1.
[434] Goldblat J. and Bernauer T., 'Proposals for Strengthening the Biological Weapons Convention', (*Bulletin of Peace Proposals*, 1991), 22(2), pp. 235-240.
[435] United Nations, 'Forth Review Conference of the Parties to the Convention on the Prohibition, the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction: Report of the Committee of the Whole', Geneva, (1996), Available at: <https://docs-library.unoda.org/Biological_Weapons_Convention_-_Fourth_Review_Conference_(1996)/BWC_CONF.IV_06.pdf>, (accessed 14 June 2022).

laboratories focusing on warfare agents. This represents a serious omission since biotechnology advances now allow for the production of toxic substances in facilities not easy to identify[436].

An incongruous fact is the lack of obligation among new Members to declare their possession of prohibited weapons. Nor are those who declare such possession required to prove that any of it has been destroyed or diverted toward peaceful purposes[437].

All in all, the absence of international means has been filled with domestic technical instruments which, however, are not sufficient to verify other countries' hostile development and production of biological agents[438]. Besides, UN Secretary General's investigations are generally carried out following suspicious reports on the possible use of chemical or biological weapons to demonstrate illegal possession, they may however prove incomplete because both the similarities between naturally occurring or deliberately caused diseases and the difficulties in identifying the aggressor[439]. This shortcoming disincentivizes states from taking on credible commitments of compliance[440].

Consultation and cooperation are two of the main duties States undertake when ratifying the Convention[441]. It derives the right to address complaints – containing all possible evidence[442] - of Convention violations to the UN Security Council. However, while a few States suffer from a lack of resources to collect the evidence required, some others cannot count on foreign or allies' sources, which results in deliberate neglect of other States' transgressions[443]. The Security Council may thus reject a request for consideration from a state suspecting a violation but lacking credible information to prove its point.

The Council itself is not tasked with compliance powers to enforce arms control agreements nor with judicial punishment powers against violators[444]. Only when a violation is suspected to lead to

[436] Lentzos F., 'Compliance and Enforcement in the Biological Weapons Regime', (*United Nations Institute for Disarmament Research*, 2019), pp.2-10.
[437] Goldblat J., 'The Biological Weapons Convention - An overview', (*International Review of the Red Cross*, 1997), pp.258.
[438] Salisbury D., 'UNSCR 1540 Implementation: Challenges Past and Present' in Stewart I., Viski A., and Salisbury D., *Preventing the Proliferation of WMDs: Measuring the Success of UN Security Council Resolution 1540*, (Palgrave Macmillan, 2018), pp. 81-83.
[439] Dembek Z.F., Kortepeter M.G., Pavlin J.A., 'Discernment between deliberate and natural infectious disease outbreaks', (*Epidemiol Infect*, 2007), 135(3), pp. 353-561.
[440] Beard J., 'The Shortcomings of Indeterminacy in Arms Control Regimes: The Case of the Biological Weapons Convention', (*The American Journal of International Law*, 2007), 101(2), pp.291-293.
[441] United Nations, 'Convention of the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction', Geneva, (1971), 1015 UNTS, entry into force 26 March 1975, Art.5.
[442] United Nations, 'Convention of the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction', Geneva, (1971), 1015 UNTS, entry into force 26 March 1975, Art.6.
[443] CSIS, 'The Biological Weapons Threat and Nonproliferation Options: A Survey of Senior U.S. Decision Makers and Policy Shapers', (*CSIS*,2006), pp. 32-34.
[444]Ibidem.

international friction, Chapter VI of the UN Charter requires the implementation of "*appropriate procedures or methods of adjustment*"[445]. Yet, this isn't' always the case.

The BWC was originally designed to address active substances with harmful health effects. Nonetheless, the existing legal shortcomings analysed above, along with recent biotechnology advances and democratize aspects of biotech R&D and production are boosting toward a more holistic approach. States Parties have suggested the negotiation of a comprehensive legally binding instrument[446] - complementing the Convention - with a greater focus on economic and technological development and compliance mechanisms. At present, however, no progress has been made so far.

3.1.4. The United Nations Security Council Resolution (UNSCR) 1540

Recent events have shown the increasing proliferation and use of weapons of mass destruction (WMD) among non-state actors, becoming one of the gravest threats to international peace and security. Since the events of 9/11, the subsequent terrorist attacks have demonstrated global criminal networks with the intent to cause death and destruction. This threat perception has been heightened by public terrorist groups' statements announcing the desire to acquire WMD[447]. Most concerning is the proliferation of WMD through clandestine networks, underling non-state actors' multiple roles in exporting and supplying weapons and technologies. The inadequacy of the traditional international WMD non-proliferation framework to address new international security issues has encouraged the United Nations Security Council, to adopt in 2004 Resolution 1540, implementing controls over the creation and delivery of WMD in order to detect their acquisition by terrorists and other non-state actors[448]. It defines binding obligations covering all three weapon types and it applies to all States, irrespective of whether they have joined multilateral non-proliferation agreements[449].

Three main lines of action include (*i*) the denial of any type of support – whether financing, transport or logistics - to non-state actors, including terrorists, engaging in proliferation activities; (*ii*) the national commitment to criminalize "*any proliferate activity*"[450], including WMD acquisition or development, and "*in any of its forms*"[451]; (*iii*) finally, the implementation of preventive and proactive measures to detect, combat illicit trafficking and proliferation by non-state actors. The Resolution

[445] United Nations, 'Charter of the United Nations', San Francisco, (1945), 1 UNTS XVI, entry into force 14 October 1945, Art.33.
[446] Feakes D., 'The Biological Weapons Convention', (*Revue scientifique et technique*, 2017), 36(2), pp. 621-628.
[447] Blum A. and others, 'Nonstate Actors, Terrorism, and Weapons of Mass Destruction', (*International Studies Review*, 2005), 7(1), pp. 165-168.
[448] UN Security Council, 'Security Council resolution 1540', (2004), S/RES/1540.
[449] Rehman H. and Qazi A., 'Significance of UNSCR 1540 and Emerging Challenges to its Effectiveness', (*Strategic Studies*, 2019), (39, 2), pp. 50-52.
[450] UN Security Council, 'Security Council resolution 1540', (2004), S/RES/1540, Preamble.
[451] Ibidem.

thus called on States to enact effective measures, introduce export controls and enhance law enforcement efforts, formulating national action plans through which map out the priorities for implementing the Resolution's key provisions[452].

The content of UNSCR 1540 has been further reinforced by other Resolutions, namely UNSCR 1673[453], UNSCR 1977[454] and UNSCR 2325[455].

Despite some successful results, most countries have not yet implemented all resolution's prescriptions and proscriptions, whose ambiguous wording makes their understanding relatively hard. This piecemeal approach risks encouraging governments to make minimal compliance efforts, while attaining little progress in enhancing global control over WMD[456]. Compounding to this fragmented scenario are the institutional and political limitations to the Security Council's action in pressing States to fill the most critical gaps in the Resolution's implementation[457].

The comprehensiveness of 1540 Resolution poses technical, legal and political issues for its implementation, which requires joint and coordinated efforts. Deterring the acquisition of WMD by non-state actors largely depends on the States' capacity to assume this responsibility. Nevertheless, numerous factors, whether political o technical, detract States from their obligation, negatively impacting the effectiveness of the resolution itself[458]. One of the major challenges obstructing governments in their core responsibilities is the lack of domestic legislation and enforcement mechanisms. Even when States agree with the Resolution's goal, they must equally prove their technical, legal expertise to implement the resolution's provisions[459].

Besides States' capacity, governments' priorities play a central role. States experiencing internal instability, hunger, or external wars are more likely to address resources and political attention to internal dynamics. In other words, the perception of the WMD terrorism threat and of illicit trafficking varies significantly across countries, limiting the establishment of 1540's controls[460].

All these factors prevent States lacking specific legal and technical capabilities from fulfilling demanding obligations, thus limiting their action to the enactment of basic measures. This is clearly

[452] Asada M., 'Security Council Resolution 1540 to Combat WMD Terrorism: Effectiveness and Legitimacy in International Legislation', (*Journal of Conflict & Security Law*, 2008), 13(3), pp. 309.
[453] UN Security Council, 'Security Council resolution 1673', (2006), S/RES/1673.
[454] UN Security Council, 'Security Council resolution 418', (1977), S/RES/418.
[455] UN Security Council, 'Security Council resolution 2325', (2016), S/RES/2325.
[456] Crail P., 'Implementing UN Security Council Resolution 1540: A Risk-Based Approach', (*Nonproliferation Review*, 2006), 13(2), pp. 356.
[457] Ibidem.
[458] Schneider J., 'The BWC's Prohibition of Biological Weapons: Reality or Rhetoric? ', (*Journal of Biosecurity, Biosafety, and Biodefense Law*, 2014), pp. 191-195.
[459] Dunworth T., Mathews J.R. and McCormack T., 'National Implementation of The Biological Weapons Convention', (*Journal of Conflict & Security Law*, 2006), 11(1), pp. 93-118.
[460] Forest J., 'Framework for Analyzing the Future Threat of WMD Terrorism', (*Journal of Strategic Security*, 2012), 5(4), pp. 51-68.

evident in numerous national progress reports[461] lacking any indication of internal legal measures to address non-state actors. No agreement on an obligation hierarchy ignores the question of the importance of each fulfilment for the Resolution's goal, thereby disincentivizing States to improve their efforts[462].

Unless States cooperate to strengthen their capacity, the Resolution's effectiveness will remain limited, allowing non-state actors to exploit the holes in the existing non-proliferation regime.[463]

The interpretation and degree of compliance with the Resolution's requirements might vary across States, where political and ideological considerations influence the central decisions on domestic legal mechanisms to adopt. Since monitoring the actual implementation in each's country judicial and executive systems at the national level is an extremely resourceful and time-consuming task, the relevant Committee is left with no choice but to count on national reports for monitoring and examining the progress made. Yet, besides not meeting the required standard, reports result biased in favour of highlighting compliance trends, while hiding non-compliance areas[464].

Although all the reports pursue the purpose of providing information transparently, their credibility is called into doubt since they include inaccurate or missing data. It follows that compliance cannot be assumed from the only submission of the report. This is further exacerbated by both the absence of consistent criteria for verifying Parties' compliance, and the ineffectiveness of enforcement measures[465].

One of the most debated issues is the vagueness of the terms – in terms of feasibility and relevance and evaluation - which doesn't provide clear guidelines on how to address specific situations or cases[466]. Firstly, Resolution 1540 fails to address the urgency of those countries particularly vulnerable to the threats of WMD proliferation. States like Japan and South Korea with ongoing nuclear programmes are at higher risk and thus would require more extensive and appropriate measures. Secondly, although binding on all States, Resolution 1540 doesn't adequately take into account the different stages of development, the number of resources available for use, the technological progress, and the technical expertise of states, all factors that impact the degree of compliance. This all-inclusive approach fails to consider the challenges resource-constrained

[461] States are required to submit periodically to the 1540 Committee detailed reports on the measures taken to fulfill the Resolution's requirements.
[462] Crail P., 'Implementing UN Security Council Resolution 1540: A Risk-Based Approach', (*Nonproliferation Review*, 2006), 13(2), pp. 359.
[463] Ibidem, pp. 358.
[464] Rehman H. and Qazi A., 'Significance of UNSCR 1540 and Emerging Challenges to its Effectiveness', (*Strategic Studies*, 2019), 39, (2), pp. 55.
[465] Crail P., 'Implementing UN Security Council Resolution 1540: A Risk-Based Approach', (*Nonproliferation Review*, 2006), 13(2), pp. 558.
[466] Gahlaut S., 'United Nations Security Council Resolution 1540 Implementation: More of the Same or Brave New World? ', (*Strategic Trade Review*,2019), 5(7), pp.55-56.

countries face when adopting implementation measures. Notwithstanding the aid and outreach to support developing nations in building capacity, there is still an uneven distribution of resources among areas.

Finally, the resolution includes a broad methodology for states' performance assessment, mostly relying on national reports. The neglect of timelines implementation results in a flawed estimate of compliance. In other words, the analysis of the existing legislation and enforcement systems should be extended to the dates of the implementation schedule, which would provide information on the time needed, providing, in turn, some estimates on the difficulties in implementing specific measures suggested by the resolution itself[467].

Overall, Resolution 1540 has contributed positively to the goal of global security, reducing the threats of WMD proliferation and terrorism. However, confusion and scepticism on compliance, prioritization, and applicability issues, along with the changing international context make the effectiveness performance difficult to evaluate.

3.2. Biological weapons and the dual-use concept

The twentieth century witnessed a colossal development of advanced weaponry with seemingly genuine and strategic advantages. Security researchers have since devoted their efforts to assessing whether new technologies and breakthroughs in life science are beneficial to society or will trigger long-term side effects[468]. Although acknowledging the extensive impacts of sequencing and synthetic technologies on economic growth and global stability, the same developments are claimed to spawn "*new opportunities for inappropriate and malicious use*"[469], potentially leading, in the worst-case scenario, to the "*transformation of life sciences into death sciences*"[470]. Countering the misuse of dual-use technology is, thus, a key goal in combating the proliferation of WMD. Recent efforts to develop nuclear and chemical weapons in Iran, Libya and Syria demonstrate the inadequacy of the existing international control systems in deterring state-sponsored initiatives that leverage dual-use technology for military ends, increasingly exacerbating the tension between scientific knowledge and security concerns[471].

[467] Rehman H. and Qazi A., 'Significance of UNSCR 1540 and Emerging Challenges to its Effectiveness', (*Strategic Studies*, 2019), 39(2), pp. 50.
[468] Rappert B., 'Why has not there been more research of concern? ', (*Public Health*, 2014), pp. 1-2.
[469] Verdirame G. and Bencic H. M., 'The Synthetic Biology Dilemma: Dual-use and the limits of academic freedom', in Gow J. and others, *Routledge Handbook of War, Law and Technology*, (Routledge, 2019), pp. 251.
[470] Atlas R.M. and Dando M., 'The dual-use dilemma for the life sciences: Perspectives, conundrums, and global solutions' (*Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, 2006), 4(3), pp. 276–286.
[471] Reichart J.F. and Caves, J., 'The Future of Weapons of Mass Destruction: their Nature and Role in 2030', (*Center for the Study of Weapons of Mass Destruction*, 2014), pp. 31-38.

Such an issue is wrapped up in the dual-use dilemma, which encompasses "*biological research with legitimate scientific purpose, the results of which may be misused to pose a biologic threat to public health and/or national security*"[472]. Unlike the traditional military-civilian connotation, the dual-use concept is now employed to distinguish benevolent research from harmful applications[473].

A clear illustration of the dual-use dilemma is open communication in science. For the benefits of science, innovation and intellectual communication, scientific data are released in open-access journals and databases. Some of these data, though, might make it easier to create a new generation of biological weapons[474]. The question arises whether the potential risks warrant a restriction on intellectual freedom and scientific progress[475]. This dilemma is best summarized in the Buddhist temple saying: " *to every man is given the key to the gates of heaven. The same key opens the gate of hell*"[476].

The dual-use conundrum entered debates over weapons and technology exports after World War II and the atomic bombings of Hiroshima and Nagasaki in 1945, when the double potential of uranium enrichment plants as a source of energy and as a nuclear explosive material drew significant resources worldwide in the attempt to improve national enrichment capabilities. Initially framed from an arms control outlook, dual-use technologies for both military and civilian applications have raised security concerns about the control and diffusion of advanced weaponry, opening discussions on scientists' social responsibility and political activity[477]. The changing nature of politics, science and political violence have recently shifted science's conception toward an industrial perspective, highlighting the exploitation of research and manufacturing efforts beyond their original purpose[478]. Although the command-and-control logic regulated and delimited technologies and research activities, the rush for technological superiority has made controlling information flow even more challenging[479].

[472] National Science Advisory Board for Biosecurity, 'National Science Advisory Board for Biosecurity Charter', (2004).
[473] Oltmann, S., 'Dual-Use Research: Investigation Across Multiple Science Disciplines', (*Science and Engineering Ethics*, 2015), 21, pp. 327–341.
[474] Smith J.A. and Sandbrink J.B., 'Biosecurity in an age of open science', (*Plos Biology*, 2022), 20(4), pp.2-5.
[475]Yim Guo R. D., 'Ethical Theory for Dual-Use Dilemmas in Synthetic Biology', (*Asian Bioethics Review*, 2012), 4(2), pp.150-159.
[476] Selgelid M.J. 'A tale of two studies: ethics, bioterrorism, and the censorship of science', (*Hastings Center Report*, 2007), pp. 35-43.
[477] Rychnovská D., 'Governing dual-use knowledge: From the politics of responsible science to the ethicalization of security', (*Security Dialogue*, 2016), 47(4), pp.314-315.
[478] Godin B., *Innovation Contested: The Idea of Innovation over the Centuries*, (Routledge, 2015), pp. 133-138.
[479] Rychnovská D., 'Governing dual-use knowledge: From the politics of responsible science to the ethicalization of security', (*Security Dialogue*, 2016), 47(4), pp. 313.

In other words, the dynamic concept of dual-use mirrors the varying concerns on data and technology misuse arising across times, emerging first in fields of cell biology and molecular, while recently extending to other areas such as ICT[480] and neurotechnology[481].

Biology and nuclear science have a comparable destructive output, although the former has shown greater potential for good. Of course, nuclear innovations have been equally employed for the peaceful production of radioactive elements – in particular, radioisotopes – and energy. However, while dual-use nuclear applications have traditionally been kept hidden for the purpose of preventing their potential misuse, biological sciences discoveries have not been similarly constrained, and knowledge-sharing has become part of the norm. In other words, when nuclear weapons technology was first developed, States restricted both information and material access, yet the same approach is doomed to fail if applied in the biotechnology field, partly because of the democratisation of life sciences and the benefits it offers to human welfare, which make it difficult to limit its expansion[482].

Life sciences have been increasingly exposed to security concerns in the 90s, in conjunction with an increase in terrorism, and then even more strenuously after the 9/11 attacks, as the US security strategy shifted toward new vulnerabilities and political violence[483]. These events have shaped current debates on biological science, which have progressively focused on the need to secure research and innovation from abuse by unpredictable actors. Framed in the war on terror narrative, these concerns stem from earlier discussions about biotechnology advances and the need to define new regulations. In the 70s, the emergence of genetic engineering and the fears of potential side effects resulted in a temporary study ban, which encouraged researchers to voluntarily agree on common safety guidelines for recombinant DNA research at the 1975 international meeting in Asilomar, marking the science's ability to govern itself[484] through self-regulation and risk-assessment practices[485].

Although military history shows multiple examples of scientific research being used intentionally or unintentionally to develop weapons, recent technological revolutions in genetics, biotechnology and synthetic biology have made it a greater threat to human existence, marking a critical juncture for policymaking and ethical decision-making in the life sciences. Recent events, including the AUM

[480] Langley, C. and Parkinson, S. 'The Political Economy of Military Science', in Tyfield D., Lave R., Randalls S. and Thorpe C., *The Routledge Handbook of the Political Economy of Science*, (Routledge, 2017), pp. 194–209.
[481] Ienca M., Jotterand, F. and Elger, B.S., 'From Healthcare to Warfare and Reverse: How Should We Regulate Dual-Use Neurotechnology?', (*Neuron*, 2018), 97, pp. 269–274.
[482] Miller S., Selgelid M., 'Ethical and Philosophical Consideration of the Dual-use Dilemma in the Biological Sciences', (*Science and Engineering Ethics*, 2007), 13, pp.549-550.
[483] National Research Council, 'Biotechnology Research in an Age of Terrorism: Confronting the Dual Use Dilemma', (*National Academy Press*, 2004).
[484] Hindmarsh R. and Gottweis, 'Recombinant regulation: The Asilomar legacy 30 years on'. (*Science as Culture*, 2006), 14(4), pp. 299–307.
[485] Jonsen A.R., *The Birth of Bioethics*, (Oxford University Press, 2003), pp. 325-351.

Shinrikyo religious cult that released nerve gas sarin at multiple locations in the Tokyo subway in the spring of 1995 and the 2001 anthrax attacks in Washington, D.C., and New York City, have made the risk from bioterrorism more tangible, raising simultaneously serious concerns and fears about the open publication of dual-use research (DURC)[486].

Compounding the dilemma surrounding technology applications is the easier access to biological, chemical and nuclear technologies by military, civilian and non-state actors. Advanced methods of genetic engineering and biotechnology have shown great potential to enhance the virulence and transmissibility of naturally occurring viruses, which raises the chances of terrorists with minimal microbiological training accessing pathogens with enhanced virulence and for which no vaccines have been developed yet[487].

New classes of technical advanced in synthetic genomics have further intensified the problem. Indeed, pathogens may now be created *ex novo*, meaning that they can now be designed from scratch, with no longer need to be looked for in inhospitable regions or to be stolen from secure laboratories[488].

In more recent publications, the debate surrounding potentially risky biomedical research is framed in the so-called 'Gain-of-function Research'[489] (GOFR), a technique altering the functions of biological agents, increasing their transmissibility and virulence[490]. Unlike DURC, the newly term GOFR refers to both biosecurity and biosafety issues, finally triggered in 2014 after the US biomedical agency started funding research on risky pathogens.

The complexity and uncertainty surrounding dual-use research and its potential uses and impacts make the management of related concerns even harder[491]. Three main shortcomings have been highlighted so far. First of all, the dual-use definition shows some limitations which hamper the anticipation and reflection on potential research uses. Secondly, the involvement and support of researchers are essential requirements for effective dual-use research governance structures. The major obstacle lies, however, in researchers' ignorance of dual-use issues, which is largely explained by the exclusion of ethical and social challenges in science education programmes or in research

[486] Rohden F., 'Proceedings of the Dual Use Research of Concern Panel Discussion: challenges and perspectives', (*Canadian Journal of Microbiology*, 2022), pp. 377-382.
[487] Galatas I., 'The misuse and malicious uses of the new biotechnologies', (*Annales des Mines - Réalités industrielles*, 2017), pp. 103-108.
[488] Yen-Hsiang W. and others, 'Synthetic biology: advancing the design of diverse genetic systems', (*Annual Review of Chemical and Biomolecular Engineering*, 2013), pp.8-10.
[489] This expression was first applied to describe two contentious studies on the H5N1 avian influenza virus, and it was then used to particular coronavirus trials.
[490] Selgelid M.J., 'Gain-of-function research: ethical analysis', (*Science and Engineering Ethics*, 2016), 22(4), pp. 923–964.
[491] Ienca M. and Vayena E., 'Dual use in the 21st century: emerging risks and global governance', (*Biomedical Intelligence*, 2018), pp. 2-5.

career frameworks[492]. Although awareness-raising activities have been increasingly promoted, they require further adapting to the specificities of each scientific discipline and research area.
Finally, the third issue highlights the urgent need for global collaboration for tackling dual-use research issues since scientific knowledge crosses national and regional borders and research goes global[493].

3.2.1. The dual-use dilemma in the biological sciences: ethical risks

A series of scientific discoveries[494] published early in the 21st century triggered a substantive debate on public health and security implications[495], allocating responsibilities among a variety of actors – notably scientists, research institutions, national governments and international bodies - who can influence the conduct and dissemination of potentially risky scientific endeavours[496]. At present, regulations governing dual-use technologies include both informal and legally binding, engaging a variety of actors sharing a culture of responsibility and awareness. The major difficulty in their implementation lies in identifying the items with a dual-use character, which further complicates the discussions about the regulation of biomedical research. Thus, developing effective regulatory measures to avoid the misuse of science and technology relies largely on the subject of such rules. Three different categories of dual-use items have been suggested so far, which include "*material, technology and knowledge*"[497] or "*research, technologies and artefacts*"[498]. However, there is still no agreement on a general definition covering all scenarios and technologies, which further complicates the safety and security risks assessment.

In managing security-related research, some scientists called for a complete ban on research publications or, at least, a partial omission of materials and methods descriptions, while some others stressed the potential benefits outweigh the risks[499]. As scientific openness and knowledge sharing

[492] Vinke S., Rais I., and Millett P., 'The Dual-Use Education Gap: Awareness and Education of Life Science Researchers on Nonpathogen-Related Dual-Use Research', (*Health Security*, 2022), 20(1), pp. 36-38.
[493] Ulnicane I., 'The governance of dual-use research in the EU: the case of neuroscience', in Antonio Calcara, Raluca Csernatoni and Chantal Lavallée, *Emerging Security Technologies and EU Governance*, (Routledge, 2020), pp. 177-191.
[494] Major scientific breakthroughs include autonomous vehicles, the Internet of Things, nanorobots, artificial intelligence and innovative molecular biology techniques.
[495] Ienca M., Effy V., 'Dual use in the 21st century: emerging risks and global governance', (*Swiss Medical Review*, 2018), pp. 1-2.
[496] Rosenstock L. and Lee L.J., 'Attacks on Science: The Risks to Evidence-Based Policy', (*Ethics and Public Health*, 2002), pp.1-4.
[497] Kuhlau F. and others, 'A precautionary principle for dual-use research in the life sciences', (*Bioethics*, 2011), 25(1), pp. 1–8.
[498] Forge J., 'Responsible Dual Use', in Rappert B. and Selgelid M.J., *On the dual uses of science and ethics. Principles, practices and prospects* (Australian National University E-Press, 2013), pp. 121–32.
[499] Miller S., Selgelid M., 'Ethical and Philosophical Consideration of the Dual-use Dilemma in the Biological Sciences', (*Science and Engineering Ethics*, 2007), 13, pp. 557.

have profound implications for progress, limiting publications and descriptions of methods would interfere with the essential science processes, namely replication and verification. Yet, it would be naïve to trust the same scientific community to self-regulate itself about dual-use issues. Suffice it to think of the great number of high-profile scientists moving from developed democratic nations to authoritarian regimes who have been engaged in WMD programs, thus being directly responsible for the development of those weapons[500].

Of remarkable importance is thus the ethical nature of key decisions posed by dual-use research, involving issues on responsibilities, benefits, harms and values. Ethical decision-making is however not always straightforward. Relevant actors, on one side, will take actions to promote the beneficial development and use of scientific knowledge, while on the other, they will endorse measures to counteract the malicious use of science, which might occasionally include avoiding the dissemination of potentially dangerous information. As scientific research is more likely to be equally beneficial and harmful, it is inherently problematic to accomplish both aims at once. It follows that a *laissez-faire* approach may support scientific innovation and the advantages therefore provided while resulting in the publication of particularly risky research, whereas a more restrictive strategy could stop the creation and/or spread of hazardous knowledge while simultaneously limiting helpful scientific advancement.

The multilayer nature of the DURC phenomenon makes the identification of emerging ethical issues no easy task. Generally framed within the clash between the principles of research freedom and research independence versus the obligation to avoid causing injury, the ethical debate on DURC touches numerous scientific fields with impacts on scientists, institutions, political bodies and society[501]. The first ethical question researchers have been focusing on is whether a potential biological threat agent should be directly eliminated or not retrieved, which would consequently result in the removal of research as no biological agent is to be explored any longer. Here, the main practical difficulty is *"to predict the consequences of knowledge prior to obtaining that knowledge*"[502], posing a challenge for *ex-ante* risk assessment exercise[503]. In this regard, the ongoing debate is all about

[500] Selgelid, M.J., 'Dual-Use Research Codes of Conduct: Lessons from the Life Sciences', (*Nanoethics*, 2009), pp. 178-180.
[501] Ehni H.J., 'Dual use and the ethical responsibility of scientists', (*Archivum Immunologiae et Therapiae Experimentalis*, 2008), 56(3), pp. 147–152.
[502] J. Kempner, J. F. Merz and C. L. Bosk, 'Forbidden knowledge: public controversy and the production of nonknowledge', (*Sociological Forum*, 2011), 26(3), p. 479.
[503] While destructionists have suggested a non-retrieval approach, arguing that stocks of live viruses are not indispensable for protecting against future outbreaks, retentionists favour a retention approach, claiming that basic research on specific live agents could provide new insights into the viral infection process and the human immune system.

finding a balance between the desirability of retaining the virus for scientific purposes versus the risks involved with not killing it.

The second question refers to biological agents whose current and/or future existence is given for sure[504]. The main issue involves unanticipated negative outcomes deriving from beneficial research, potentially resulting in the weaponization of a specific pathogen and a consequent biological attack. Finally, the third issue focuses on whether to conduct dual-use research for defensive purposes against weaponised agents. While analysing pathogenicity and dispersion mechanisms is an essential step in developing defences capabilities against a putative BW agent, deeper comprehension of these elements is precisely what would facilitate the creation of a virulent novel pathogen and its subsequent weaponization.[505]

Multilateral treaties including the Biological Weapons Convention (BWC) and the 1925 Geneva Protocol[506] prohibit the development, production, and storage of biological weapons and mandate the destruction of existing weapons, while missing concrete recommendations for the subnational or national levels. One reason for this gap lies in the drawback governmental regulation poses to academic freedom, scientific autonomy and freedom of speech, elements that all contribute to the progress of science[507].

Furthermore, of crucial importance is academic freedom, generally referred to as the "*freedom of members of the academic community, assembled in colleges and universities, which underlies the effective performance of their functions of teaching, learning, practice of the arts, and research*"[508]. Although it is not explicitly mentioned in the United Nations Covenants on Human Rights[509], many scholars believe academic freedom is comparable to an international right deriving from the freedom of expression and opinion and the right to education[510]. While the latter is guaranteed in Art.19 of the Universal Declaration of Human Rights[511] (UDHR) and in all the major international human rights treaties – notably in Art. 19 of the International Covenant on Civil and Political Rights[512], Art. 10 of

[504] For instance, research into whether avian influenza may start a human pandemic could result in the development of hazardous new strains potentially exploited by terrorists.
[505] Miller S., Selgelid M., 'Ethical and Philosophical Consideration of the Dual-use Dilemma in the Biological Sciences', (*Science and Engineering Ethics*, 2007), 13, pp. 549-550.
[506] Cited above, pp. 13-15.
[507] Buchanan A. and Kelley M.C., 'Biodefence and the production of knowledge: rethinking the problem', (*Journal of Medical Ethics*, 2013), 39(4), pp. 195–204.
[508] Fuchs R.F., 'Academic freedom: its basic philosophy, function, and history', (*Law and Contemporary Problems*, 1963), 28, p. 431.
[509] UN General Assembly, 'International Covenants on Human Rights', New York, (1996), A/RES/50/171.
[510] Vrielinka J. and others, 'Academic Freedom as a Fundamental Right', (*Procedia Social and Behavioral Sciences*, 2011), pp. 117-141; Wright J., Avouris A., Frost M. and Hoffmann S., 'Supporting academic freedom as a human right: challenges and solutions in academic publishing', (*The International Journal of Human Rights*, 2022), pp. 1-3.
[511] UN General Assembly, 'Universal Declaration of Human Rights', New York, (1948), 217 A (III), Art.19.
[512] UN General Assembly, International Covenant on Civil and Political Rights, New York, (1966), 999 UNTS 171, entry into force 23 March 1976, Art. 19.

the European Convention on Human Rights[513], Art. 13 of the American Convention on Human Rights[514], and Art. 9 of the African Charter on Human and Peoples' Rights[515] - the right to education is equally ensured in the UDHR and in Art. 13 of the International Covenant on Economic, Social and Cultural Rights[516]. As a non-absolute value, academic freedom is however subject to limitation clauses - including national security above all – whenever its exercise clashes with other fundamental rights. Accordingly, the responsibility of a scientist to freely share his results might be overridden when a contingency such as a pandemic or terrorist attacks, arises. Censorship of academic freedom thus requires specific justification detailing the potential risks of misuse associated with a research project outcome[517].

Yet, the right to security's ambiguity has been largely exploited with serious implications. Indeed, while it "*encapsulates, on one hand, a commitment to rights, which we commonly associate with absence from coercion"* on the other, it includes *"a commitment to coercion in the name of individual and collective security*"[518].Unfortunately, no case law from international human rights courts helps to understand how to weight demands of national security and academic freedom in the area of dual risk[519].

In short, the right to research and exchange sensitive information is reasonably restricted in cases of national security and public health implications. Prudence is, however, highly requires since, "*restrictions on academic freedom are a defining feature of authoritarianism*"[520].

Although the DURC's ethical dilemma may actually be useful in particular learning contexts, it shows several drawbacks[521]. First of all, the existing framing does not help to understand how the scientific community views and addresses the dual-use issue. If organizations and scientists ignore the dilemmas they face, they are likely to remain unconscious of potential questions of concern. As the ultimate goal of DURC regulation and governance is the prevention of potentially catastrophic

[513] Council of Europe, 'Convention for the Protection of Human Rights and Fundamental Freedoms', Rome, (1950), ETS 5, entry into force 3 September 1953, Art.10.
[514] Organization of American States (OAS), 'American Convention on Human Rights', Costa Rica, (1969), 1144 UNTS 123, entry into force 18 July 1978, Art. 13.
[515] Organization of African Unity (OAU), 'African Charter on Human and Peoples' Rights', Banjul, (1981), CAB/LEG/67/3 rev. 5, 21 I.L.M. 58, entry into force 21 October 1986, Art.9.
[516] United Nations, General Assembly, 'International Covenant on Economic, Social, and Cultural Rights', New York, (1966), 993 UNTS 3, entry into force 3 January 1976, Art.13.
[517] B. Rajagopal, 'Academic freedom as a human right: An internationalist perspective', (*Journal of the American Association of University Professors*, 2003), 89(3), p. 29.
[518] Dickinson R., 'The Right to Security - Securing Rights or Securitising Rights', (*Oxford Legal Studies Research Paper*, 2013), pp. 89.
[519] Verdirame G. and Habian M.B., 'The Synthetic Biology Dilemma: Dual-use and the limits of academic freedom', in Gow J., Dijxhoorn E., Kerr R., Verdirame G., *Routledge Handbook of War, Law and Technology*, (Routledge, 2019), pp. 258.
[520] Ibidem.
[521] Edwards B., and others, 'From cases to capacity? A critical reflection on the role of 'ethical dilemmas' in the development of dual-use governance, (*Science and Engineering Ethics*, 2014), 20(2), pp. 571–82.

occurrences, the dilemma framing tactic is ineffective if it cannot encourage the relevant stakeholders to engage proactively.

Secondly, defining a 'dilemma' involves deeper political discussions about the institutional framework and operational procedures of biotechnology. The politics of regulating DURC may be hampered in the long run if dual-use issues are predominantly debated case by case as a series of challenges. Instead, politics should operate anticipatorily and at a higher political level. Therefore, describing DURC as an ethical conundrum does not necessarily help with the development of effective policies that are embraced by the relevant parties.

Lastly, DURC regulation issues differ from conventional perspectives of a dilemma where research practice is either fully allowed or completely prohibited. Rather, comprehensive analyses that thoroughly weigh each specific case of research conduct, together with its potential ramifications for the law, ethics, and society are highly required[522].

Overall, the broad range of ethical and legal issues related to scientific research is urging the implementation of a new and updated strategy regulating emerging technologies and potential risks.

[522] Salloch S. 'The dual use of research ethics committees: why professional self-governance falls short in preserving biosecurity', (*BMC Medical Ethics*, 2018), pp.3-4.

Chapter 4

Toward a hybrid defence

4.1. The Converging Risk Landscape

The strategic studies community has shown sustained interest in the analysis of computing power, automated systems, hypersonic technologies and AI advances. While some expect these and other emerging and disruptive technologies (EDTs) to revolutionize conventional and unconventional warfare capabilities, strategies and operations, some others accuse revolutionary optimism to be overblown, as it ignores the human factor and assumes technological innovation to provide innovative solutions to cope with unexpected crises[523]. Although the potential of biotechnology developments in shaping warfighting doctrines had been acknowledged more than twenty years ago, the scenario today is vastly different. The pace of innovation and technological change, accompanied by continued uncertainty– both about the potential risks and benefits –make forecasting a difficult task, challenging traditional remedies[524].

This debate has been unfolding in the Digital Age, where information has started converting and moving between the merging physical and digital worlds. The extraordinary growth in information and communication technologies has coincided with an increase in computing performance, accelerating digitalization trends with a significant impact on society, governments and markets. Frequently used in the field of economics, digitalization describes how information and communication technologies generate profit and value in network-based organizations, opening up opportunities and creative potential[525].

What is of relevance in security discussions is, however, the increased connectivity of systems and their enhanced management and storage capacity[526]. Although opening enormous opportunities for advancements in bioeconomy research and innovation, this hyperconnectivity has lowered barriers to access technological capabilities, broadening the risks of accidental, unintended or deliberate

[523] Fiott D., 'Digitalization and hybrid threats: Assessing the vulnerabilities for European security', (*The European Centre of Excellence for Countering Hybrid Threats*, 2022), pp. 7-10.
[524] NATO Science & Technology Organization, 'Science & Technology Trends: 2020-2040 – Exploring the S&T Edge', March 2020, Available at: <https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf>, (accessed 11 July 2022).
[525] G. Valenduc and P. Vendramin, 'Digitalisation, between Disruption and Evolution', (*European Review of Labour and Research*, 2017), 23(2), pp. 121-134.
[526] Daniel Fiott, 'Digitalising Defence: Protecting Europe in the Age of Quantum Computing and the Cloud', (*EUISS Brief*, 2020), 4(2), pp. 2-5.

misuse[527]. As a result, the bioengineering emergence across a variety of industrial sectors has made any point in the convergence of biotechnologies and IT vulnerable to cyber security attacks[528].
Declining costs and improved education have widened the poll of actors – including companies, organizations and individuals – accessing biotechnologies, know-how and material resources, exposing today's society to new hybrid risks and threats including supply disruption, data manipulation and spying[529]. It comes as no surprise the hypothesis from the European Defence Agency's most recent Technology Foresight report of a world where a multitude of actors will have unprecedented access to laboratory equipment, gene editing kits and nuclear reactors[530].
This has recently gathered the attention of the NATO Science and Technology Organization[531](STO) on the distribution issue threatening the proliferation of cutting-edge technology across potential malicious actors. The BWC secretariat raised concerns about possible BWC violations in 2018, noting that players have now more access to technologies like gene drives, gene editing, and gene synthesis with little or no monitoring from governments or established industry bodies. The decentralization of technological use thus requires greater prioritization of strong policy and control measures, reducing covert consequences governments, individuals, and businesses are increasingly exposed to.

The convergence of biological and digital information with energy, public health and the cyber realm makes any attack potentially lethal to national security[532]. The Covid-19 pandemic clearly illustrates the enormous political, social and economic costs of essential critical infrastructure threats and hazards. Strong evidence has emerged of foreign interference in the forms of industrial espionage, cyber-hacking and IP theft, with significant privacy breaches and public health outcomes[533]. Essential pillars of biosecurity policies including laboratory access, funding, control over tools and possession of critical equipment and materials have accordingly not proved their worth[534].

---

[527] Hamilton R. A., 'Opportunities, Challenges, and Future Considerations for Top-Down Governance for Biosecurity and Synthetic Biology' in Trump B, Florin M.V., Perkins E., Linkov I., *Emerging Threats of Synthetic Biology and Biotechnology: Addressing Security and Resilience Issues*, (Springer, 2019), pp. 37-40.
[528] DiEuliis D., 'Science and Technology: Parsing the Digital Biosecurity Landscape', (*Georgetown Journal of International Affairs*, 2020), pp. 166-170.
[529] Trump D., 'Synthetic Biology, GMO, and Risk: What Is New, and What is Different? ', Trump B.D., Cummings C.L., Kuzma J., Linkov I., *Synthetic biology 2020: frontiers in risk analysis and governance*, (Springer, 2020), pp. 85-87.
[530] European Defence Agency, 'EDA Technology Foresight Exercise 2021: Welcome to the Futures – Future Narratives', (2021), pp.8-9, Available at: <https://eda.europa.eu/docs/default-source/documents/202105-edatechnologyforesightexercise-futuresnarratives_v5.pdf>, (accessed 12 July 2022)
[531] It is a NATO subsidiary entity gathering engineers and scientists from Partner nations in the pursuit of the Alliance's science and technology needs by sharing and generating innovation and scientific solutions.
[532] George, A. M., 'The National Security Implications of Cyberbiosecurity', (*Frontiers in Bioengineering and Biotechnology*, 2019), 7(51), pp. 1-4.
[533] Lawless, J. and Kirka, D., 'UK, US, Canada Accuse Russia of Hacking Virus Vaccine Trials', (*TechXplore*, 2020), Available at: <https://techxplore.com/news/2020-07-uk-canada-accuse-russia-hacking.html>, (accessed 13 July 2022).
[534] O'Brien J. and Nelson C., 'Assessing the Risks Posed by the Convergence of Artificial Intelligence and Biotechnology', (*Health Security*, 2020), 18(3), pp. 225-226.

This is the result of increasing high-speed Internet availability, which has reduced prior barriers to knowledge transfers, making information hazard spillage the major concern of today's governments. Widely understood as "*the rate-limiting step that connects a normatively bad actor with the missing inspiration, knowledge, and processes to deploy scientific capabilities for harmful purposes*"[535], information hazards challenge the management of dual-use information requiring a trade-off between the benefits and the potential for harm. Through hacking cyber and bio-processing systems, criminal groups and state actors have for instance easy access to sensitive data and equipment for the production and release of hazardous and novel pathogens[536], potentially causing harm to public, plant and animal health[537].

Continuous advances in technology might, thus, increase the sophistication and accessibility of cyber and bio attacks, begging the issue of whether existing security approaches will be adequate to tackle emerging and future threats.

The global diffusion of enabling capabilities with dual use potential has significantly impacted the modus operandi of international security and conflicts, arising grey areas deliberately exploited to minimize legal, military and political consequences. Following the 2005 publication of *The rise of hybrid wars*[538] by two US military officials highlighting the convergence of conventional and unconventional tactics and the 2014 invasion of Crimea and the interplay of deniable special forces, modern hybrid warfare has gained significant prominence in policy debates[539]. Even though a common definition has not been established under international law, the term broadly describes a combination of operations and battlespaces across all five domains of cyber, space, air, maritime, land, and a blurring of actors with "*the scope of achieving strategic objectives by creating exploitable ambiguity*"[540]. In other words, a range of new technical means is combined in a synchronised manner to exploit adversaries' vulnerabilities and achieve nefarious purposes in a context of non-obvious warfare engaging a complex mix of non-state and state actors. Emerging and disruptive technologies have given hybrid war a new quality, further undermining existing international framework ensuring

[535] Bostrom N., 'Information hazards: a typology of potential harms from knowledge', (*Review Contemporary Philosophy*, 2011), pp. 44–79.
[536] In March 2003, the capture of Khaled Sheikh Mohammed, an operational planner for al-Qaeda, by the CIA has revealed the organization purchased the equipment required for the production of botulinum bacteria and developed a spread plan.
Barton G., 'Al Qaeda Near Biological, Chemical Arms Production', (*Washington Post*, 2003), Available at: < https://www.washingtonpost.com/archive/politics/2003/03/23/al-qaeda-near-biological-chemical-arms-production/8b88e5d0-5f00-4b3c-83a8-b396c0856d90/>, (accessed 29 August 2022).
[537] Bajema, N., DiEuliis, D., Lutes, C., & Lim, Y., 'The Digitization of Biology: Understanding the New Risks and Implications for Governance', (*Center for the Study of Weapons of Mass Destruction*, 2018), pp. 17-18.
[538] Hoffman F., and Mattis J., Future Warfare: The Rise of Hybrid Wars, (*Potomac Institute for Policy Studies*, 2005).
[539] James K. Wither, 'Defining Hybrid Warfare', (*Journal of European Security Defense*, 2020), 10(1), pp. 7-9.
[540] Cormac R. and Aldrich R., Grey is the new black: covert action and implausible deniability, (*International Affair*s, 2018), 94(3), pp. 477–494.

territorial integrity and state sovereignty. Their major advantage is to be employed below the threshold of armed conflict, deriving political and military benefits while raising ambiguity and attribution issues[541]. The common way this is achieved is through a covert action. Although reasons for undertaking covert actions may vary, States have increasingly adopted hybrid strategies exploiting the weakness of the international enforcement regime, casting doubts on the legality of their behaviour.

Several factors suggest current security and defence methodologies are deficient in comprehending existing and upcoming vulnerabilities to the bioeconomy. Firstly, existing threat/risk models have long been centred on tacit knowledge and the malicious use of new biotechnologies. This aspect has however become less important given the increasing accessibility to biological data and know-how[542]. Tacit knowledge involves expertise, training and social collaboration scientists gain working in laboratories. Conventional assumptions supposing malicious actors need biology training are no longer valid. Recent advances in integration and automation of biological life have indeed developed new "*attack vectors and risks*"[543] no longer depending on tacit knowledge, suggesting the reconsideration of its impact. It is, however, made somewhat difficult by the lack of awareness among researchers and scientists of the increasing severity of attacks, further exacerbated by inadequate expertise and training. This motivates controversies on what life science information should be labelled risky and how to control them.

This is further complicated by divergent biosecurity and cybersecurity practices worldwide. Since the US and Europe are no longer the leading nations in advanced research, new approaches to bio and cyber security have emerged, with different degrees of tolerances and constructions of risks[544]. Newcomers to the development of innovative cyber and bio techniques have raised two main implications. The first entails varying safety and security procedures at various points of the global supply chain, while the second includes the chance for experiments or national biosecurity regulations to evade the authority of a State, spreading across political boundaries. This poses serious concerns when the environmental impacts of a specific biology application deemed acceptable in one country spread into another country, disrupting local ecologies and exposing vulnerable populations to unavoidable negative effects[545].

---

[541] Thiele R., *Hybrid Warfare Future and Technologies*, (Springer, 2021), pp.1-5.
[542] Mueller S., 'Facing the 2020 Pandemic: What Does Cyberbiosecurity Want Us to Know to Safeguard the Future? ' (*Biosafety and Health*, 2020), pp. 11-21.
[543] Ulven J.B., Wangen G., 'A Systematic Review of Cybersecurity Risks in Higher Education', (*Future Internet*. 202), 13(2), pp. 39.
[544] Russia, China and Saudi Arabia are three main newcomers to the field.
[545] Trump B., Florin M.V., Perkins E. and Linkov I., Biosecurity for Synthetic Biology and Emerging Biotechnologies: Critical Challenges for Governance in Biology' in Trump B, Florin M.V., Perkins E., Linkov I., *Emerging Threats of Synthetic Biology and Biotechnology: Addressing Security and Resilience Issues*, (Springer, 2019), pp. 5-7.

Secondly, what complicates the understanding of emerging hybrid threats is the sheer magnitude of the bioeconomy and the number of public and private organizations involved. The growing reliance and combination of communication, computation and physical processes can easily lead to both purposeful and inadvertent malevolent biological outcomes. Threats and dangers of all types can take different forms at any point in the production process[546]. Accordingly, the complexity of biomanufacturing processes makes the assessment and identification of threat actors and associated risks increasingly challenging.

Overall, the biotechnology convergence with AI is turning into a geostrategic asset to strengthen a nation's digital sovereignty and preserve both domestic and global security. However, the lack of proper institutional and legal frameworks, can create vulnerabilities and insecurity flashpoints, challenging health, food and civilian security. The digital transition, thus, requires a broader security analysis that is not confined to malicious activities but includes questions on critical infrastructure, legislation, energy management, critical supply chain and raw materials.

4.2. Hybrid threats and human rights obligations: filling the legal gaps

Over three decades ago, the end of the Cold War spread a sense of hope and optimism toward a more cooperative, democratic, and liberal international order finally replacing great power rivalry and ideological differences[547]. This enthusiasm was rapidly swept away by civil uprisings, failed states, and growing ethnic tensions, dashing hopes for a peaceful global order. These setbacks have started questioning the existing world order and the role of international and intermediary organizations in great powers' relations[548].

Debates on the changing security panorama have been further fuelled by recent trends towards national antagonistic approaches[549]. This is clearly visible in 2014 Russia's unexpected invasion of the Crimean Peninsula and its subsequent annexation, widely condemned as an act of aggression and violation of the international system and its principles of territorial integrity, sovereign equality and political independence[550]. Similarly, China has increasingly adopted a more assertive approach towards its maritime claims and interests over the South China Sea, disputing the judgement by the

[546] For instance, risks faced by a biotech firm will differ from those faced by a medical sciences company or a multinational food company that produces genetically modified foods.
[547] Fukuyama F., *The End of History and the Last Man*, (Free Press, 1992), pp. 189-190.
[548] Pert A., 'International Law in a Post-Post-Cold War World—Can It Survive? ', (*Asia and the Pacific Policy Studies*, 2017), 4(2), pp. 362-375.
[549] Sari A., 'Hybrid threats and the law: Concepts, trends and implications', (*The European Centre of Excellence for Countering Hybrid Threats*, 2020), pp. 8-9.
[550] Grant D.T., *Aggression against Ukraine: Territory, Responsibility, and International Law*, (Palgrave Macmillan, 2015), pp. 15.23.

Permanent Court of Arbitration[551]. In tandem, recent unilateral withdrawals from international institutions and agreements – notably the Philippines' decision to leave the International Criminal Court[552] and the United States' removal from several international agreements, including the Iran nuclear deal[553] - witness a growing mistrust of global norms and procedures, thus challenging the traditional support for a rules-based international system[554].

This shift towards increasing unilateralism and open hostility has been followed by globalization trends and major technological advancements resulting in greater availability and potential for technology application. Yet, the wide accessibility and easy acquisition has allowed a greater number of nations and non-State actors to access new and potentially devastating due-use technology, while simultaneously generating new opportunities of unwanted foreign influence in the common guise of false news, electoral intervention, and cyber espionage, exposing modern communities to terrorism, hostile influence, and foreign meddling[555].

Overall, two interconnected phenomena are marking the evolution of today's security environment: first, the intensification of the great powers' geostrategic competition - largely made possible by new technological advances - and second, the mounting pressure on international norms, institutions, and procedures designed to contain geopolitical rivalry. While some believe these events demonstrate the illusion of a rules-based international system[556], others consider these trends a call for renewable efforts toward multilateralism[557].

What is beyond dispute is the serious threat these developments pose to the international rule of law. The turn to geopolitical antagonisms has indeed resulted in selective compliance and grave breaches of international law's core principles[558] , whose application has become part of a strategic operating

[551] Statement of the Ministry of Foreign Affairs of the People's Republic of China on the Award of 12 July 2016 of the Arbitral Tribunal in the South China Sea Arbitration Established at the Request of the Republic of the Philippines, (*Chinese Journal of International Law*, 2016), 15(4), pp. 905-907.
[552] Gutierrez J., 'Philippines Officially Leaves the International Criminal Court', (*New York Times*, 2019), Available at: < https://www.nytimes.com/2019/03/17/world/asia/philippines-international-criminal-court.html>, (accessed 14 July 2022).
[553] Mulligan S., 'Withdrawal from International Agreements: Legal Framework, the Paris Agreement, and the Iran Nuclear Agreement', (*Congressional Research Service*, 2018), Available at: < https://sgp.fas.org/crs/row/R44761.pdf>, (accessed 16 July 2022).
[554] Stokes D., 'Trump, American Hegemony and the Future of the Liberal International Order', (*International Affairs*, 2018), 94(1), pp. 145-147.
[555] Gronvall G., Biosecurity: the opportunities and threats of industrialization and personalization, (*Bulletin of the Atomic Scientists*, 2015), 71(6), pp. 39–44.
[556] Sari A., 'Hybrid threats and the law: Concepts, trends and implications', (*The European Centre of Excellence for Countering Hybrid Threats*, 2020), pp. 8-9.
[557] Krueger A., 'An enduring need: multilateralism in the twenty-first century', (*Oxford Review of Economic Policy*, 2007), 23(3), pp. 335-346; Nelli Feroci F., Greco E. and Pirozzi N., 'Renewing Multilateralism for the 21st century: the Role of the United Nations and of the European Union', (*IAI*, 2020), pp. 6-9, Available at: <https://www.iai.it/sites/default/files/9782930769455.pdf>, (accessed 30 August 2022).
[558] Evidence suggests major breaches affect international human rights law, *jus in bello* and *jus ad bellum*.

environment[559]. Generally, domestic and international law is employed to regulate roles and behaviours and to sanction perpetrators in case of gross violations through the exercise of coercive power. Recent trends show, however, growing use of lawfare practices, generally understood as "*the strategy of using—or misusing—law as a substitute for traditional military means to achieve an operational objective*"[560]. Indeed, there is a raising tendency to enforce the law to justify national conducts, highlighting substantive weaknesses of the international legal system and its enforcement mechanisms[561]. Compliance is indeed a key source of legitimacy, which explains why governments tend to mask their non-conformal behaviour rather than admit it[562].

To further exacerbate this situation is the inherent ambiguities and uncertainties of legal systems. This frequently results in ambiguous interpretations of the law, unclear roles and responsibilities and a relative incapacity of lawmakers to foresee unusual situations. Although legal grey areas provide certain benefits, they also open up tremendous opportunities for hostile actors in their strategic interests[563].

In virtue of their sovereign status, states can indeed act freely in the international arena in accordance with the *Lotus principle*[564], as long as their actions are not forbidden by any relevant principles of international law. This has, for instance, significant implications for information and other influence operations. Although they may amount to a threat of force[565] expressly forbidden under Article 2(4) of the United Nations Charter, it is improbable that they amount to an actual use of force, unless they cause damage or physical injury[566]. Indeed, only interventions producing kinetic damage are labelled

[559] Cogan J., 'Noncompliance and the International Rule of Law', (*The Yale Journal of International Law*, 2006), 31, pp. 189-193.
[560] Dunlap C., 'Lawfare Today: A Perspective', (*Yale Journal of International Affairs*, 2008), pp. 146.
[561] Kennedy D., *Of War and Law* (Princeton University Press, Princeton, 2006), pp.33-39.
[562] A notable instance is Russia's annexation of Crimea. Responding to the charges of violating international law, the Russian President claimed the legitimacy of its military forces on the Crimean Peninsula based on bilateral agreements between Ukraine and Russia. Although this is true, the arrangement of its troops beyond the agreed military bases is an unambiguous violation of pre-existing negotiations;
Socher J., *Russia and the Right to Self-Determination in the Post-Soviet Space*, (Oxford University Press, 2021), pp. 151-160.
[563] Morris L. and others, *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*, (Rand Corporation, 2019), pp. 1-7.
[564] Hertogen A., 'Letting Lotus Bloom', (*The European Journal of International Law*, 2016), 26(4), pp. 901-906.
[565] Influence Operations include the acquisition of strategic information about an adversary, as well as disinformation activities to gain competitive advantage over an opponent. Although the difficulties in identifying specific circumstances where Influence Operations are prohibited under Articles 2(4), the Nicaragua case determined that influence efforts in overthrowing another state's government constitute a violation of Article 2. This is indeed perceived as a violation of the principle of non-intervention. The prohibition of intervention does not include force as a necessary element under Article 2(4). Yet, the lack of state practice leaves the thresholds and conditions of its violation still unclear.
[566] The historical application of Article 2(4) suggests drafters intended the prohibition of the use of force to apply to physical means of force causing damage and physical harm to another country.

as an unlawful use of force, which demonstrate the inability of the present article to protect States from new methods of hybrid warfare[567].

As the aforementioned article excludes non-physical acts, these operations are likelier to be governed by the principle of non-intervention, which forbids foreign interference that aims to force the targeted State into "*matters in which each State is authorized, by the principle of State sovereignty, to decide freely*"[568]. However, it raises two controversial issues including both (1) what prohibited coercion consists of and (2) the threshold prohibiting non-coercive interference. This legal vagueness allows States to undertake offensive influence operations without being constrained by norms or running the danger of facing unfavourable legal repercussions.

In armed conflicts warfare tactics and means – among which energy and autonomous weapons, cyber warfare and drone technologies - have generated moral and humanitarian considerations[569]. Finding common ground on control measures and/ or weapons restrictions has thus been challenging. One of the main reasons is disagreement, insofar, conflict contexts have raised contentious questions on needs, visions, aspirations and strategies. A second influencing factor is uncertainty. Indeed, although controls are reasonably simple to implement in the early phases of a technology's development, the lack of demonstrable evidence of harm makes them difficult to justify[570]. When artillery, tanks and chemical weapons were first developed, their innovative potential was believed to quickly end wars, minimizing both combatant and non-combatant casualties. Nonetheless, once acknowledged the need for controls and safeguards, their implementation has been far more challenging and expensive because of their robust integration into military procedures and routines. As a matter of fact, the evolving nature of war, along with the shifting narratives and tools used to assess the legitimate use of physical force challenge the introduction of restrictions on armed force's means. Leading factors include the waning importance of state-to-state conflict and how new technological capabilities obscure what constitutes an armed conflict[571].

In response to increasing situations labelled as '*military operations other than war*[572] *(MOOTW)*', there has been a growing effort to advance new norms in international human rights law prioritizing

[567] Buchan R., 'Unlawful Uses of Force or Prohibited Interventions? ', (*Journal of Conflict and Security Law*, 2012), 17(2), pp. 214.
[568] International Court of Justice (ICJ), 'Case Concerning Military and Paramilitary Activities in and against Nicaragua', (Nicaragua v. United States of America), 27 June 1986, para. 205.
[569] ICRC, 'New technologies and warfare', (*International Review of the Red Cross*, 2012), 94(886), pp. 483-500, Available at: < https://www.icrc.org/en/doc/resources/international-review/review-886-new-technologies-warfare/review-886-all.pdf>, (accessed 17 July 2022).
[570] Rappert B., 'Can the Law Regulate the Humanitarian Effects of Technologies? ', in Gow J., Dijxhoorn E., Kerr R., Verdirame G., *Routledge Handbook of War, Law and Technology*, (Taylor and Francis, 2019), pp. 50-55.
[571] Stewart D., 'New Technology and the Law of Armed Conflict', (*International Law Studies*, 2011), pp. 271-275.
[572] The acronym was coined in the 90s by the U.S. military.

the right to life during wartime. As embodied in IHL, armed conflicts are required to balance military necessity and humanity (as well as property) concerns, thus limiting the right of parties to choose whatever warfare means or methods[573]. Although controls over conflict means and methods are laid out in a number of specific legal norms – notably provisions prohibiting indiscriminate attacks[574] , as well as rules governing the legal use of force in an armed conflict[575] and requiring parties to a conflict the respect of the precautionary principle in attack and defence[576] – their sufficiency has been subject to contentious debates. The difficulty of evaluating military benefit and civilian harm on a case-by-case basis makes a particular regime of arms control hard to justify[577], as they might be challenged by specific incidents where technological weaponry does not cause deleterious effects.

That being said, nuclear weapons perfectly illustrate the complexity of establishing restrictions through international law. In 1994, the International Court of Justice was asked for an advisory opinion on whether the threat or use of nuclear weapons would necessarily breach the tenets and norms of international humanitarian law[578]. In the final opinion, judges acknowledged the lack of a universal prohibition or authorization of the threat of use of nuclear weapons[579]. It was further claimed that this use must adhere to the principles and rules of international law[580]. However, the Court did not conclude with certainty that "*the use of nuclear weapons would necessarily be at variance with the principles and rules of law in any circumstance*"[581], leaving unsolved questions on its categorical lawfulness. Hence, although the use and threat to use nuclear weapons were generally agreed to be against international law, this has not been defined as always valid. As no legal ruling or consensus enshrines their categorical unacceptability, the latter has been derived from the Biological Weapons Convention, the Geneva Protocol and other official statements[582]. This belief is set against the rules of IHL and any other parts of international law that allow the proportionate and discriminate use of

Britschgi A., 'Military Operations other than War: Coming in from the Cold' in Magyar K., *United States Post-Cold War Defence Interests*, (Palgrave Macmillan, 2004), pp.150-153.

[573] Cohen A. and Zlotogorski D., *Proportionality in International Humanitarian Law: Consequences, Precautions, and Procedures*, (Oxford University Press, 2021), pp, 22-36.

[574] The rule of proportionality requires a careful analysis of consequential loss or damage and the military advantage of potential attacks against a legitimate object.

[575] This is summed up in the principle of distinction, which allows direct attacks only against on groups and objects constituting the armed forces of a party involved in the conflict, while it guarantees protection to the civilians from the effects of the hostilities.

[576] Henckaerts Jean-Marie Louise Doswald-Beck Carolin Alvermann and International Committee of the Red Cross, *Customary International Humanitarian Law*. (Cambridge University Press, 2005), Rule 15.

[577] Schmitt M., 'Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance', (*Virginia Journal of International Law*, 2010), pp. 796-798.

[578] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, July 8, 1996, ICJ Rep. 1996.

[579] Ibidem, para. 74.

[580] Ibidem, para. 22.

[581] Ibidem, para. 95.

[582] Henckaerts J-M., and Doswald-Beck L., *Customary International Humanitarian Law*, (Cambridge University Press, 2004), pp.256-258.

specific forms of bioweapons. The lack of clear rules raises reasonable worries about the proliferation of laboratory equipment and techniques to many more individuals and non-governmental groups[583].

Besides acknowledging the challenges associated with warfare governance, it's equally relevant to consider the potential dangers deriving from the categorical prohibition of biological weapons[584]. Exceptionalism theorists, for instance, believe norms reinforce beliefs about what is right and what is wrong, producing accepted standards where unconventional weapons – meaning biological, nuclear and chemical weapons – are deemed cruel as they kill differently from traditional weapons. This approach risks ignoring the destructive potential of conventional weapons – comparable to small nuclear weapons – which are not however subject to the same level of scrutiny[585].

Furthermore, the risks of potential long-term war harm on the environment, and thus on the existence of individual human beings and communities, have increasingly become a subject of international debates[586]. First awareness came after the serious environmental damages caused in the Vietnam War (1955-1975), encouraging the rapid development of international legal instruments[587]. Yet, one of the first challenges the protection of the environment in armed conflict faced has been the applicability of the law itself. While the laws of war were first developed in a time of international armed conflicts (IAC), today's world is overwhelmed by a growing number of non-international armed conflicts (NIAC) - mostly involving non-governmental armed groups - causing the greatest damage to the environment[588]. Overall, as almost every violent activity brings about some negative environmental impacts, it raises the question of how much environmental damage is forbidden. Articles 35(3) and 55 of the Additional Protocol I (API) ban the use of warfare methods causing "*widespread, long-term, and severe*"[589] harm to the natural environment. Nevertheless, besides the uncertainty around these terms, the three criteria are hardly possible to meet, defining a bar that is unreasonably high[590]. What exacerbates this vagueness is the unsolved question of whether the mentioned articles apply to

[583] Tucker J., *Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies*, (MIT Press, 2012), pp. 17-19.
[584] Rappert B., 'Can the Law Regulate the Humanitarian Effects of Technologies? ', in Gow J., Dijxhoorn E., Kerr R., Verdirame G., *Routledge Handbook of War, Law and Technology*, (Taylor and Francis, 2019), pp. 56-59.
[585] Tannenwald N., *The Nuclear Taboo*, (Cambridge University Press, 2007), pp. 317–324.
[586] Sjöstedt B. and Dienelt A., 'Enhancing the Protection of the Environment in Relation to Armed Conflicts: Draft Principles of the International Law Commission and beyond', (*Goettingen Journal of International Law*, 2020), pp.13-25.
[587] First efforts include the Environmental Modification Convention (*ENMOD*) in 1978 – later renamed Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques, the first Additional Protocol (*API*) and the World Charter for Nature (1982).
[588] Leins K., *New war technologies and international law: the legal limits to weaponizing nanomaterials*, (Cambridge University Press, 2022), pp. 125-126
[589] International Committee of the Red Cross (ICRC), *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, Art.35(3).
[590] Verwey W., 'Observation on the Legal Protection of the Environment in Times of International Armed Conflict' in Kiss A.C. and Lammers J., *Hague Yearbook of International Law*, (Brill, 1994).

non-member States of the API – notably the United States which objected to the environmental provisions as being broad and vague[591].

The rapid technological advancements have made this situation even more critical. Nanomaterials and their dual-use potential clearly illustrate this point. The main challenging feature is the invisible nature and the little understanding of how these weapons affect the human body—whether by inhalation, digestion, or absorption – and the potential impact on the environment. Although early investigations started soon after the Vietnam War, none of the current international environmental legal instruments makes any reference to nanomaterials, questioning the adequacy of existing control measures in facing emerging risks[592].

Similarly, international human rights principles are requiring careful consideration. Historically, the two legal regimes, the *jus in bello* and the *just ad bellum* were kept separate, meaning that the laws of war were understood to apply to all cases of declared war, whereas human rights were drafted to apply in times of peace[593]. This mutually exclusive distinction has raised numerous issues in the evolution of laws. As no surprise, none of the first human rights instruments – including the Magna Carta (1215), the English bill of Rights (1689) and the French Declaration on the Rights of Man and Citizen (1789) - make reference to weapons, or more broadly, wars. The only remark was found in Article 20 of the International Covenant on Civil and Political Rights (ICCPR), noting that "*any propaganda for war shall be prohibited by law*"[594].

Over the past twenty years, human rights law has been progressively extended to armed conflicts because of the broad protection it offered to civilians[595]. Yet, as the laws of war were traditionally understood to limit and prohibit permanent harm – such as death or disability - during armed conflict, new technologies and emerging weapon capabilities with long-term health effects call for a legal re-evaluation under Article 36[596] to reflect compliance with human rights principles[597].

New biological abilities to manipulate life and living organisms at the nanoscale have recently raised serious and complex ethics issues, urging a broader analysis of long-term implications for human

[591] Roberts G., 'The New Rules for Waging War: The Case against Ratification of Additional Protocol', (*Virginia Journal of International Law*, 1985), pp.125-126.
[592] Schmitt M., 'Green War: An Assessment of the Environmental Law of International Armed Conflict', (*Yale Journal of International Law*, 1997), 22(1), pp. 71-73.
[593] Leins K., *New war technologies and international law: the legal limits to weaponising nanomaterials*, (Cambridge University Press, 2022), pp. 166.
[594] UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, UNTS 999, 16 December 1966, New York, entry into force 23 March 1976, Art. 2
[595] Schoiswohl M., 'Human Rights and Disarmament – A Blind Date or Shotgun Marriage? ', (Austrian Review of International and European Law, 2013), 15(1), pp. 116-119.
[596] Leins K., *New war technologies and international law: the legal limits to weaponising nanomaterials*, (Cambridge University Press, 2022), pp. 192-194.
[597] Murray D. and others, *Practitioners' Guide to Human Rights Law in Armed Conflict*, (Oxford University Press, 2016), pp. 165- 179.

health. In the year 2015, a new genetic project introduced a unique engineering technique called CRISPR-Cas9[598], offering revolutionary advances in the prevention and treatment of diseases, in the production of chemicals and fragrances and in the understanding of gene function. Although earlier genome editing techniques have facilitated the generation of mutant genes through knockout, knock-in or mouse models[599], the most recent scientific development has provided a more reliable, accessible and cost-effective approach applying today in numerous biological research, from plant modification, human disease and animal models. In other words, CRISPR's technology allows the intentional alteration of human genomes that would pass down to subsequent generations, potentially changing the genetic makeup of humans. This has raised bioethical concerns about the possibility of genetic modification being exploited as a welfare method, bypassing regulatory controls[600].

Although both the CWC and the BWC constrain germline modification, the newest technique's feasibility makes it easily accessible to multiple actors - including non-state bodies - thus urging the implementation of hybrid regulatory models. The main challenge lies however in the different national perspectives: countries' legal systems are required to evolve, including emerging technologies' risks in national frameworks, and thus facing the question of what is already covered and what is not[601]. Much of the issue builds upon the novelty attributed to synthetic biology. Numerous jurisdictions actively pursuing synthetic biology research do not make any explicit reference to it in legal documents. The Research Office of Parliament in Germany, for instance, concluded that current synthetic biology practices fall within conventional biotechnology and thus are already covered by existing regulations[602]. Neither EU legislation contains any mention of synthetic biology as it generally takes a very long time to update its biosafety standards due to different perspectives on the necessity and desirability of change[603].

The various national regulatory frameworks governing synthetic biology and biosecurity are fragmented in multiple pieces of legislation – covering bioweapons, technologies, dual-use materials, human health, agriculture, export/import and transport, and criminality - and are only addressed

[598] The acronym CRISPR means Clustered Regularly Interspaced Short Palindromic Repeats, while Cas9 refers to the bacterial enzyme involved in immune response.
[599] Mansour S.L., Thomas K.R., Capecchi M.R., 'Disruption of the proto-oncogene int-2 in mouse embryo-derived stem cells: a general strategy for targeting mutations to non-selectable genes', (*Nature*, 1988), pp. 348–352.
[600] Ayanoğlu F., Elçin A., Murat Elçin Y., 'Bioethical issues in genome editing by CRISPR-Cas9 technology', (*Turkish Journal of Biology*, 2020), pp.110-120.
[601] Fenwick M., Kaal A. W., Vermeulen E., 'Regulation Tomorrow: What Happens When Technology Is Faster than the Law? ', (American University Business Law Review, 2017), 6(3), pp. 583-585.
[602] Krink N., Löchner A., Cooper H., Beisel, C. and Di Ventura B., 'Synthetic biology landscape and community in Germany', (*Biotechnology Notes*, 2022), 3, pp.8-14.
[603] Eriksson D. and others, 'A welcome proposal to amend the GMO legislation of the EU', (*Trends in Biotechnology*, 2018), 36(11), pp. 1100–1103.

indirectly[604]. Taking the example of Finland, more than 20 acts and regulations cover aspects of biosafety and biosecurity, although none specifically mention synthetic biology. Unlikely, in the US, there are over 35 different biosecurity regulations explicitly mentioning synthetic biology.
Some other countries, instead, lack relevant bio and cyber security regulations. This is especially the case of developing countries where resources are mostly addressed to human rights and food security issues[605].

The nature and effect of international agreements may thus create a false impression on the level of adoption and consensus. Conventions' effectiveness depends instead on the commitment from all countries to adapt and implement effectively legal measures, which may require a considerable amount of time. For instance, although GMO regulations have a relatively long history, still not all nations have enacted relevant legislative instruments.
National implementation adheres to geographical and legal practice areas, aiming to shape and influence domestic audiences' behaviours. This is a key for robust global governance where all States cooperate to mitigate the risks deriving from scientific and technological advancements[606].
The convergent nature of synthetic biology, for instance, may arise ambiguities on which rules to apply and how to regulate specific developments. This could potentially result in regulatory redundancies, or worse, in accountability gaps as States tend to dump responsibility on one another. Meanwhile, divergencies in biological processes and methods may become too broad to regulate individually, which might cause increasing duplication and fragmentation of national laws[607].

4.3. Suggestions for potential future developments from a legal perspective

Cyber-bio weapons are increasingly gathering international attention. While it's now reasonable to assume that sub-state organizations', individuals' or non-state actors' cyber biological capabilities wouldn't be sufficient to cause large numbers of casualties, this may possibly change as civilian and commercial research continue to advance. The lack of effective and coordinated interventions raises concerns over both the proliferation of laboratory tools and agents and advances in life sciences

[604] Greer S.L., Trump B., 'Regulation and regime: the comparative politics of adaptive regulation in synthetic biology', (*Policy Science*, 2019), 52(4), pp. 505–524.
[605] Hamilton R.A., Mampuys R., Galaitsi S.E., Collins A., Istomin I., Ahteensuu M., and Bakanidze L., 'Opportunities, Challenges, and Future Considerations for Top-Down Governance for Biosecurity and Synthetic Biology', in Trump B, Florin M.V., Perkins E., Linkov I., *Emerging Threats of Synthetic Biology and Biotechnology: Addressing Security and Resilience Issues*, (Springer, 2019), pp. 50-52.
[606] Benedict K., 'Global Governance' in Wright J., *International Encyclopedia of the Social & Behavioral Sciences*, (Elsevier, 2012), pp. 155-161.
[607] Trump B.D., 'Synthetic biology regulation and governance: lessons from TAPIC for the United States, European Union, and Singapore', (*Health Policy*, 2017), 121(11), pp. 1139–1146.

information and techniques, urging a common normative standard that encourages community-oriented policing, preventing biology from being put to malign use[608].

Doing this requires legal practitioners to engage with science and technoscientific issues to the extent they can consciously govern them and participate in high-level panel discussions. Although sounding obvious, this means keeping abreast of scientific research advances and approaching those areas of law that do not necessarily fall within their immediate specialities – ranging from human rights law to laws of war. Amid a similar vein, lawyers have the critical function to raise fundamental questions with the goal of strengthening the existing legal frameworks and highlighting legal limits, suggesting creative methods of governance and codes of conduct. This is absolutely key in ensuring good governance in future and effective compliance as technological innovation continues to change our lives and challenge existing legal frameworks and western narratives[609].

Simultaneously, scientists, technologists and engineers are required a basic understanding of current legal systems and normative constraints, to ensure their scientific advancements do not conflict with international law[610]. The International Committee of the Red Cross (ICRC) has suggested universities provide specific training on national and international law, risks, and scientists' legal and ethical responsibilities "*to prevent the hostile use of their research and its practical applications*"[611], with the overall goal of establishing a common culture of compliance and responsibility[612]. In other words, education is meant to foster scientists' understanding of their social responsibility through a deep overview of their work's implications and risks. Active learning implying simulations and scenario-based practical examples helps enhance critical analysis and assessment and contribute to further awareness of biosecurity and biosafety risks. Continued development training allows research centres to develop a strong safety and security culture to minimize potential modern technology accidents[613]. This entails common mechanisms, procedures, attitudes and practices ensuring risks are adequately identified, addressed and successfully managed across the research and innovation cycle[614].

---

[608] Rappert B., 'Why has not there been more Research of Concern?, (*Frontiers in Public Health*, 2014), pp. 6-11.
[609] Goding V., Tranter K., 'The machine runs itself: law is technology and Australian embryo and human cloning law', (*Griffith Law Review*, 2021), 30(2), pp. 240-269.
[610] Rappert B. and McLeish C., *A Web of Prevention: Biological Weapons, Life Sciences, and the Governance of Research*, (Routledge, 2014), pp. 4.
[611] Pennisi E., 'Robotic Stingray Powered by Light Activated Muscle Cells', (*Science*, 2016), Available at: <https://www.science.org/content/article/robotic-stingray-powered-light-activated-muscle-cells>, (accessed 20 July 2022).
[612] International Committee of the Red Cross, 'Functional Perspective on the Biological Weapons Convention and Chemical Weapons Convention', (2006), Available at: <https://www.icrc.org/en/doc/resources/documents/statement/biological-chemical-weapons-statement-111206.htm>, (accessed 20 July 2022).
[613] Roberts K., 'New Challenges in Organisational Research: High Reliability Organisations', (*Industrial Crisis , Quarterly*,1989), 3(2), pp. 111–125.
[614] Revill J., Husbands J., and Bowman K., *Governance of Dual Use Research in the Life Sciences: Advancing Global Consensus on Research Oversight*, (The National Academies Press, 2018), pp. 37-43.

Besides the expertise of lawyers, reviews of technologies of warfare require collaborative relationships between different scientific fields, including engineering, physics, mathematics, computer science, chemistry, materials science, and many more.

Although life sciences have always shown the potential for both maleficent and beneficent purposes, the conventional distinction between security and civilian uses has become increasingly blurred. A new array of genomic technologies has expanded the opportunities for modifying human biology, raising social, legal and ethical concerns[615]. Although regulators acknowledge the need to balance exploratory risk research and regulatory measures, the question of how to deal with new scientific information and risks remains unanswered. It is thus important to involve the scientific community "*throughout the rule-making process to prevent excessive restrictions that are potentially counter-productive to national biosecurity*"[616].

While some authors believe regulations should not hinder innovation[617], some others call for stricter regulations throughout the development process[618]. The latter approach is favoured to reduce access to materials, equipment and knowledge to engage in synthetic biology, lowering the risks of intentional or unintentional harmful research[619]. It's however important that research does not stop simply because of the unknown risks it may encounter in the future.

Governments might, simultaneously, start by strengthening the existing prohibitions and introducing materials at the nanoscale within the existing frameworks of the BWC and the CWC, stimulating the predictability and stability of the law. This requires all nations to find common practices when dealing with advanced biotechnology. Indeed, while regulations on bioweapons are objectively perceived as fair, much of modern advanced technologies lie in grey zones because of their dual-use potential.

As cyber and bio capabilities keep evolving and threats expanded, experts have thus suggested new international agreements[620]. In addition to some new forms of international governance, nations are called to build and strengthen their preparedness strategies – meaning their capacity to respond to

[615] Leins K., *New war technologies and international law: the legal limits to weaponizing nanomaterials*, (Cambridge University Press, 2022), pp. 194-216.
[616] Baskin C.R., 'Who should be driving US science policy? ', (*Perspectives in Biology and Medicine* ,2019), 62(1), pp. 20–30.
[617] De Beer J. and Jain V., 'Inclusive innovation in biohacker spaces: the role of systems and networks', (*Technology Innovation Management Review*, 2018), 8(2), pp. 27–37.
[618] Gomez-Tatay L., Hernandez-Andreu J.M., 'Biosafety and biosecurity in synthetic biology: a review', (*Critical Reviews in Environmental Science and Technology*, 2019), 49(17), pp. 1587–1621.
[619] Diggans J., Leproust E., 'Next steps for access to safe, secure DNA synthesis', (*Frontiers in Bioengineering and Biotechnology*, 2019), pp. 86.
[620] Greer S.L., Trump B., 'Regulation and regime: the comparative politics of adaptive regulation in synthetic biology', (*Policy Science*, 2019), 52(4), pp. 505–524.

potential biosecurity threats and carry out effective responses - through a combination of soft and hard law instruments[621].

In this respect, one shall always consider that technology generally adapts to societal changes more quickly than the law[622]. This is not, however, an excuse to undervalue or ignore the applicable law. Additionally, there is frequently a veil of secrecy around methods and processes used in military-industrial production and scientific research[623]. Unintended consequences of the secrecy surrounding certain nanomaterials' creation might increase public mistrust and worry about military and non-military advancements.

Beyond doubt are the precious contributions of scientists, industry representatives and academic communities in developing knowledge on new technologies' risks. Equally relevant is the role of non-governmental and intergovernmental organisations in ensuring the implementation and enforcement of international laws across multiple regimes[624]. The lack of consensus on specific issues may however delay the outcomes and challenge international understanding.

As academic disciplines employ different terminology representing diverse cultural backgrounds, agreeing on a common language to communicate efficiently and sharing information is key. Active and constructive interaction among the numerous stakeholders is thus crucial for identifying creative solutions and reconciling conflicting interests. Collaboration between experts is also claimed to reduce biosecurity threats, as it allows gathering the best available data from numerous sectors, developing a strong sense of self-regulation and ethics among scientists [625].

Multiple legal frameworks governing modern international law show duplication and overlapping tendencies, which develops conflicting legal standards, further highlighting the fragmented and occasionally conflicting character of international legal activity. The International Law Commission (ILC) published a research study on the fragmentation of the law in 2006, claiming that much of international law was accompanied by its own 'ethos'[626]. In many cases, it is difficult to reconcile the various legal frameworks because of this 'ethos' across legal regimes, which has been the subject of

[621] Nelson M., Roffey P., 'McNevin D., Lennard C., Gahan M.E., 'An overview of biosecurity in Australia', (*Australian Journal of Forensic Sciences*, 2014), 46(4), pp. 383–396.
[622] Susskind R., *The Future of Law: Facing the Challenges of Information Technology*, (Clarendon Press, 1996), pp. 9-13.
[623] The Royal Society & The Royal Academy of Engineering, 'Nanoscience and Nanotechnologies: Opportunities and Uncertainties', (*The Royal Society*, 2004), pp. 55-56.
[624] Young M.A., 'Regime Interaction in Creating, Implementing and Enforcing International Law' in *Regime Interaction in International Law: Facing Fragmentation*, (Cambridge University Press, 2012), pp. 109.
[625] Suk J.E., Bartels C., Broberg E., Struelens M.J., Ozin A.J., 'Dual-use research debates and public health: better integration would do no harm', (*Frontiers in Public Health*, 2014), pp, 114-116.
[626] Study Group of the International Law Commission, 'Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law', (2016), Document A/CN.4/L.682 and Add.1, Available at: < https://legal.un.org/ilc/documentation/english/a_cn4_l682.pdf>, (accessed 26 July 2022).

extensive and sometimes intense negotiations and histories. Although this normative pluralism is reported in numerous areas, human rights and rules of war are two of the main overlapping regimes that have been extensively studied.

In this context, Young' research suggests "*a legal framework of regime interaction where there is no regime hierarchy; where the interaction between regimes is 'continuous and constant'; and where the authority of one regime is always contestable*"[627].

The laws of war, disarmament agreements, environmental law, and human rights law, among others, have all developed independently of one another, while intertwining themselves. These treaties span in the period from 1925 to 1992, include varying numbers of parties and reservations, and are frequently backed by soft law instruments. Analysing these regimes from a "*legal, historical, doctrinal, institutional, and social*" perspective is thus necessary to comprehend how they interact in hidden ways[628].

Given all the above, government officials, lawyers, and academics must equally consider the use of cyber-bio weapons by non-State entities when enacting legislation. The 1996 Forth BWC Review Conference restated the applicability of BWC prohibition on terrorist groups' acts. In 2004, UNSCR 1540 specifically included non-State actors in the list of entities subject to the Geneva Protocol, the BWC, and the CWC[629]. Furthermore, all nations are required by United Nations Security Council Resolution 1540 to desist from supporting non-State actors or providing them with dual-use materials[630]. Regardless of the efforts and resources invested, numerous signatories haven't made any step forward in guaranteeing domestic compliance with international law requirements. It follows the need to strengthen enforcement mechanisms, to further foster accountability and compliance in such a peculiar field on international law.

[627] Young M. A., 'Regime Interaction in Creating, Implementing and Enforcing International Law', in Young M.A., *Regime Interaction in International Law: Facing Fragmentation,* (Cambridge University Press, 2012), pp. 109-111.
[628] Young M.A., 'Introduction: The Productive Friction between Regimes' in *Regime Interaction in International Law: Facing Fragmentation*, (Cambridge University Press, 2012), pp. 1-2.
[629] Asada M., 'Security Council Resolution 1540 to Combat WMD Terrorism: Effectiveness and Legitimacy in International Legislation', (*Journal of Conflict & Security Law*, 2008), 13(3), pp. 305-306.
[630] UN Security Council, 'Security Council resolution 1540', 28 April 2004, S/RES/1540, para. 1.

Conclusion

The proliferation of cyber attacks has encouraged States to adopt a whole range of instruments, including technical and ethical guidelines, regulations and monitoring mechanisms, all aiming at enhancing cyber and bio security in national and global terms. Many of the normative solutions draw from existing international law principles and seek to prevent malicious activities, uphold human and privacy rights online and encourage a responsible use of ICT resources

The growing convergence of technologies has begged the issue of whether current security approaches are adequate to tackle emerging and future threats. The present analysis suggests current security and defense methodologies are deficient in tackling existing and upcoming vulnerabilities to the bioeconomy.

Besides the very little understanding of emerging technologies, their risks and potential impacts, legal systems are filled with inherent ambiguities and uncertainties, which frequently result in ambiguous interpretations of the law, unclear roles and responsibilities and a relative incapacity of lawmakers to foresee unusual situations. This is further exacerbated by the variety of actors involved in the shape and implementation of both normative and technical standards, along with the numerous values and legal instruments at play, fomenting tensions and divergencies over how challenges should be governed.

This results in limited progress and increasing non-compliance behaviours, raising concerns over the potential economic, human and societal costs of cyber and bio activities.

The digital transition, thus, requires a broader analysis exploring new legal and hybrid tools and reviewing existing procedures. This involves a significant engagement from researchers, legislators, regulators and industry actors, ensuring a more cooperative policy environment.

Finally, new issues will undoubtedly emerge, exacerbating current risks and vulnerabilities. As a result, existing legislative and governance frameworks will probably need to be modified and reviewed over time.

Summary

La quarta rivoluzione industriale – più comunemente nota come Industria 4.0 - è stata caratterizzata dalla fusione intelligente di tecnologie emergenti che combinano la sfera fisica, digitale e biologica. Cambiamenti radicali hanno interessato il tessuto economico, sociale e culturale, con promettenti vantaggi per l'industria e l'ambiente. Miliardi di dispositivi IoT- con una potenza di elaborazione ed una capacità di archiviazione senza precedenti - hanno sviluppato un potenziale illimitato, stimolato da emergenti innovazioni nel campo della robotica, dell'intelligenza artificiale, dell'Internet delle cose e delle biotecnologie, aprendo a loro volta una nuova gamma di capacità nei settori della sanità, dell'agricoltura, dell'automazione e dell'energia.

Al contempo, la nuova era ha generato una serie di preoccupazioni legate alla proliferazione di tecnologie a duplice uso. Automazione e connettività, unite ad una crescente convergenza tecnologica, hanno permesso un ampio e crescente accesso a capacità bio informatiche, moltiplicando le opportunità di attacco alla sicurezza cibernetica. Recenti indagini hanno messo in evidenza i potenziali rischi derivanti da una crescente dipendenza delle scienze biologiche da strumenti computerizzati, che si ritiene espongano dati sensibili a crescenti vulnerabilità, generando una nuova area di rischi cyber-bio. Ciò si riassume nell'emergente nozione di cyber-bio sicurezza, disciplina ibrida comprendente di cybersecurity, biosecurity e cyber-physical security, che mira ad identificare e mitigare i rischi cibernetici la cui filiera della bioeconomia è gradualmente esposta.

Parallelamente, il crescente entusiasmo per le scienze biologiche ha dato vita a movimenti sociali - come la comunità di bio hackers, comunemente nota con il nome di *biologia fai-da-te* - in cui le stesse vengono studiate e praticate con i metodi tradizionalmente impiegati negli istituti di ricerca. Informazioni, risorse e strumenti vengono scambiati liberamente, creando una buona matrice di competenza libera da specifici quadri normativi. Oltre a questioni etiche e legali, la democratizzazione della scienza è stata oggetto di critiche circa la sua qualità, integrità ed affidabilità, inasprendo l'incertezza e la complessità che circonda le questioni di bio-sicurezza. Rischi di esposizione e propagazione di agenti biologici sono amplificati da divergenze nelle pratiche di laboratorio e nelle misure di sicurezza informatica, con conseguenze potenzialmente devastati per l'ambiente e per l'uomo.

La concatenazione di tali dinamiche ha risvegliato il potenziale di agenti biologici o tossinici come strumenti di guerra, concretizzando la minaccia di bioterrorismo. La difficoltà ad individuarne la produzione e rintracciarne la disseminazione permette agli autori del fatto di rimanere anonimi, diventando estremamente attraenti ai gruppi terroristi.

I costi bassi, uniti ad una facile reperibilità delle informazioni, hanno progressivamente incentivato attori statati e non ad investire in tecnologie emergenti con potenziale dirompente, rivoluzionando le capacità belliche ed introducendo strategie di guerra ibrida. Il potenziale degli sviluppi biotecnologici ha infatti mutato irreversibilmente la natura del conflitto armato, che ha progressivamente accostato a tecniche tradizionali elementi di guerra informatica e cibernetica. L'emergente natura ibrida ha fortemente indebolito l'esistente quadro normativo, alimentando zone grigie e aprendo ampi spazi di manovra. Le missioni di hybrid warfare hanno il principale vantaggio di trattenersi al di sotto della soglia del conflitto armato, sollevando problemi di ambiguità e attribuzione giuridica.
L'incapacità del diritto internazionale di rispondere alle emergenti sfide in campo militare rischia, tuttavia, di normalizzare l'impiego di strumenti asimmetrici, alimentando l'instabilità sulla scena internazionale.

L'acuirsi delle attività malevoli nel cyberspazio, accompagnato da un numero crescente di terroristi, hacktivisti ed attori non tradizionali, ha messo a dura prova il quadro normativo internazionale, alimentando critiche e riserve.
A livello internazionale, due gli strumenti messi in campo per fronteggiare e regolare la crescente criminalità informatica. Il primo, denominato Manuale di Tallin 1.0, diretto dal Centro di Eccellenza della NATO per la Difesa Cibernetica (CCD COE), raccoglie i principi e norme del diritto internazionale applicabile alla guerra cibernetica, più recentemente aggiornato nella versione 2.0. Sebbene rappresenti un importante punto di partenza, il Manuale presenta numerose difficoltà interpretative circa la classificazione di attori non statali, i criteri per valutare un atto illecito, l'obbligo di due diligence verso terzi e prevedibilmente la protezione dei diritti umani nel cyberspazio.

Un simile sforzo è stato sostenuto dal Consiglio d'Europa con l'approvazione della Convenzione di Budapest, documento normativo disciplinante il crimine informatico. Nonostante si proponga come strumento su vasta scala, la scarsa partecipazione ne limita l'influenza ai soli 66 paesi firmatari.
Ad indebolire ulteriormente la sua efficacia, sono le persistenti divergenze tra regolamenti in materia di cybercriminalità che impediscono un'armonizzazione del settore. Dibattuta è inoltre la scarsa tutela dei diritti degli Stati, come anche degli individui.
In un clima di ambiguità ed incertezza, il diritto alla privacy e alla riservatezza hanno assunto un ruolo chiave, spingendo verso opzioni e regole che disciplinino e garantiscano la transizione e l'uso dei dati.

Oltre alle innumerevoli implicazioni collegate al cyberspazio, la convergente evoluzione dei sistemi informatici e biotecnologi ha reso fondamentale la valutazione e mitigazione degli impatti ambientali. Una prima consapevolezza è stata raggiunta con la guerra del Vietnam (1955 – 1975) e l'impiego

abusivo di armi chimiche, i cui danni ambientali hanno favorito lo sviluppo di quadri di biosicurezza che affrontassero la diffusione aggressiva di specie invasive e l'insorgere di malattie infettive, sia di origine naturale che di atti deliberati. Le recenti tendenze alla globalizzazione e i progressi tecnologici hanno esacerbato in modo significativo lo spettro delle minacce, dando progressivamente vita a partenariati regionali e internazionali e a strumenti globali volti alla non proliferazione di armi e beni a duplice impiego, sviluppando una maggiore comprensione dei potenziali rischi e delle vigenti pratiche in materia di prevenzione e sicurezza.

Gli sforzi internazionali hanno condotto a quattro fonti normative, che costituiscono oggi la spina dorsale dell'attuale regime globale di biosicurezza. In primis, la Convenzione sulla diversità biologica (CBD) del 1993, che promuove e garantisce la conservazione della diversità biologica e l'uso sostenibile delle sue componenti. In breve, la Convenzione riconosce la necessità di salvaguardare l'ambiente e proteggere la salute umana dagli effetti dirompenti delle moderne tecnologie, pur riconoscendone il promettente potenziale.
Tuttavia, principale ostacolo ad un'adeguata attuazione della stessa è spesso l'inadeguatezza istituzionale - per lo più associata a difficoltà di coordinamento tra gli organismi governativi ed una scarsa ripartizione dei ruoli e delle responsabilità tra il livello centrale e quello subnazionale - unita a limitate risorse scientifiche, tecniche ed umane ed una scarsa partecipazione della comunità scientifica.

Di altrettanto rilievo il Regolamento Sanitario Internazionale dell'OMS del 2005 (RSI) contenente una serie di obblighi strutturali volti a rafforzare le capacità di valutazione e risposta a potenziali emergenze sanitarie. I requisiti minimi imposti garantiscono parallelamente un equilibrio tra il dovere statale di garantire la salute dei propri cittadini e l'obbligo di attuare misure di protezione sanitaria che non interferiscano con il commercio internazionale.
Un approccio flessibile pervade l'intero regolamento, offrendo ai governi nazionali ampio margine di manovra nell'adozione di meccanismi appropriati al proprio contesto economico, politico e culturale. Tuttavia, lo stesso, inasprito dall'insufficienza di specifiche linee guida, rischia di incentivare sistemi di monitoraggio e segnalazione poco accurati. Ugualmente dibattuta è la mancanza di un'effettiva autorità legale che imponga l'implementazione di meccanismi minimi, la cui conformità sembra essere lasciata alla discrezione degli stati stessi.

Terzo strumento è la Convenzione sulle Armi Biologiche e Tossiniche (BTWC) del 1975, un primo accordo di disarmo multilaterale che vieta lo sviluppo, produzione e detenzione di armi batteriologiche. Oltre ad alcune ambiguità linguistiche ed interpretative, maggiormente dibattuta è l'assenza di meccanismi di conformità per verificare potenziali intenzioni ostili. Gli stati, così come

i laboratori di ricerca, non sono tenuti a notificare all'autorità competente attività che coinvolgono agenti biologici o tossine. Tale omissione è estremamente rischiosa, in quanto i progressi della biotecnologia consentono oggi la produzione di sostanze tossiche in strutture non facilmente identificabili.

Per potenziare ulteriormente gli strumenti convenzionali, il Consiglio di Sicurezza delle Nazioni Unite ha votato all'unanimità l'adozione della Risoluzione 1540, che affronta i rischi di proliferazione di armi di distruzione di massa da parte di attori non statali.
Nonostante alcuni risvolti positivi, la maggior parte dei paesi firmatari non ha ancora attuato il contenuto della risoluzione, la cui formulazione ambigua ne rende difficile la comprensione. Tale frammentarietà, esacerbata da scarse risorse e limitata cooperazione, rischia di incoraggiare i governi a compiere sforzi minimi, invertendo i progressi nel controllo sulle armi di distruzione di massa. A questo scenario, si aggiunge un inefficiente ruolo del Consiglio di Sicurezza nel sollecitare gli Stati a colmare le lacune più critiche nell'attuazione della Risoluzione.

L’intersecazione dei molteplici quadri giuridici vigenti produce una complessa sovrapposizione normativa, che determina il carattere frammentario e talvolta conflittuale del diritto internazionale. Tale incertezza sollecita l’adozione di standard comuni e armonizzati, attraverso interventi coordinati e strutturati, di fronte una continua evoluzione dei sistemi informativi e biotecnologici che continua a sollevare preoccupazioni sociali, legali ed etiche.
Nonostante le autorità riconoscano la necessità di bilanciare i progetti di ricerca con adeguate norme giuridiche, rimane irrisolto il nodo sulle emergenti tecnologie e i rischi connessi. Emerge dunque l’importanza del coinvolgimento della comunità scientifica durante l’intero processo normativo, per evitare restrizioni controproducenti alla ricerca e alla cyber- bio sicurezza.

I giuristi giocano un altrettanto ruolo chiave nel modernizzare i quadri esistenti ed evidenziarne i limiti, suggerendo al contempo metodi innovativi di governance e codici di condotta.
Oltre alle competenze dei giuristi, gli scienziati, i rappresentanti dell’industria, i ricercatori ed ingegneri sono chiamati ad una comprensione degli attuali sistemi legali e dei vincoli normativi, scongiurando ogni conflittualità tra progressi scientifici e diritto internazionale. Formazioni ad hoc volte allo studio dei rischi e responsabilità legali ed etiche degli scienziati sono promesse, con l’obiettivo di stabilire una comune cultura di conformità e sicurezza.
L'apprendimento attivo, che implica simulazioni ed esempi pratici basati su scenari, aiuta a migliorare l'analisi e la valutazione critica e contribuisce ad aumentare la consapevolezza dei rischi legati alla biosicurezza. Interessante è anche il ruolo delle organizzazioni non governative e intergovernative nel garantire l'attuazione e l'applicazione delle leggi internazionali attraverso molteplici regimi.

Inestimabile il valore della ricerca, i cui rischi non devono precludere la sua avanzata, ma stimolarne l’aggiornamento normativo.

Bibliography

Books and contributions

- Aggarwal-Khan S., *The Policy Process in International Environmental Governance*, (Palgrave Macmillan, 2011).
- Bail C. and Falkner R., *The Cartagena Protocol on Biosafety: Reconciling Trade in Biotechnology with Environment and Development,* (Routledge, 2001).
- Baumann M-O. and Schünemann W., 'Introduction: Privacy, Data Protection and Cybersecurity in Europe', in Schünemann W. and Baumann M-O., *Privacy, Data Protection and Cybersecurity in Europe* (Springer 2017).
- Benedict K., 'Global Governance' in Wright J., *International Encyclopedia of the Social & Behavioral Sciences*, (Elsevier, 2012).
- Britschgi A., 'Military Operations other than War: Coming in from the Cold' in Magyar K., *United States Post-Cold War Defence Interests*, (Palgrave Macmillan, 2004), pp.150-153.
- Cohen A. and Zlotogorski D., *Proportionality in International Humanitarian Law: Consequences, Precautions, and Procedures*, (Oxford University Press, 2021).
- Cordonier Segger M.C., Perron-Welch F. and Frison C., *Legal Aspects of implementing the Cartagena Protocol on Biosafety*, (Cambridge, 2013).
- Desai B.H., *Multilateral Environmental Agreements: Legal Status of the Secretariats,* (Cambridge University Press, 2010).
- Dignum V., *Artificial Intelligence: Foundations, Theory, and Algorithms: how to Develop and Use AI in a Responsible Way*, (Springer, 2019).
- Dunn Cavelty M. and Wenger A., *Cyber Security Politics Socio-Technological Transformations and Political Fragmentation*, (Routledge, 2022).
- E. Hey, 'The Interaction Between Human Rights and the Environment in the European Aarhus Space', in Grear A. and Kotzé L.J., *Research Handbook on Human Rights and the Environment* (Edward Elgar, 2015).
- Egziabher T., 'The Cartagena Protocol on Biosafety: History, Content and Implementation from a Developing Country Perspective', in Traavik T. and Ching L.L., *Biosafety First*, (Tapir Academic Press, 2007).
- Forge J., 'Responsible Dual Use', in Rappert B. and Selgelid M.J., *On the dual uses of science and ethics. Principles, practices and prospects* (Australian National University E-Press, 2013).
- Fukuyama F., *The End of History and the Last Man*, (Free Press, 1992).

- Grant D.T., *Aggression against Ukraine: Territory, Responsibility, and International Law*, (Palgrave Macmillan, 2015).
- Godin B., *Innovation Contested: The Idea of Innovation over the Centuries*, (Routledge, 2015).
- González Fuster G. and Jasmontaite L., 'Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights', In Christen M, Gordijn B, and Loi M, *The Ethics Of Cybersecurity* (Springer, 2020).
- Górka K., Their A. and Łuszczyk M., 'Consequences of the Fourth Industrial Revolution in Social and Economic Development in the 21st Century', in Nogalski B. and Buła P., *Industry 4.0 and Digitalization*, (Jagiellonian University Press, 2021).
- Hamilton R. A., 'Opportunities, Challenges, and Future Considerations for Top-Down Governance for Biosecurity and Synthetic Biology' in Trump B, Florin M.V., Perkins E., Linkov I., *Emerging Threats of Synthetic Biology and Biotechnology: Addressing Security and Resilience Issues*, (Springer, 2019).
- Hamilton R.A., Mampuys R., Galaitsi S.E., Collins A., Istomin I., Ahteensuu M., and Bakanidze L., 'Opportunities, Challenges, and Future Considerations for Top-Down Governance for Biosecurity and Synthetic Biology', in Trump B, Florin M.V., Perkins E., Linkov I., *Emerging Threats of Synthetic Biology and Biotechnology: Addressing Security and Resilience Issues*, (Springer, 2019).
- Henckaerts J-M., and Doswald-Beck L., *Customary International Humanitarian Law*, (Cambridge University Press, 2004).
- Jasmontaite L., and Pavel Burloiu V., 'Lithuania and Romania to Introduce Cybersecurity Laws', in Wolf J. Schünemann and Max-Otto Baumann, *Privacy, Data Protection and Cybersecurity in Europe*, (Springer 2017).
- Jennings R., and Watts A., *Oppenheim's International Law*, (Oxford, 2008).
- Jonsen A.R., *The Birth of Bioethics*, (Oxford University Press, 2003).
- Kay A. and Williams O., *Global Health Governance: Crisis, Institutions and Political Economy*, (Palgrave Macmillan, 2009).
- Kaspter A. and Mölder H., 'The EU's Common Security and Defence Policy in Facing New Security Challenges and Its Impact on Cyber Defence' in Ramiro Troitino D. and others, *The EU In The 21St Century* (Springer, 2020).
- Kennedy D., *Of War and Law* (Princeton University Press, Princeton, 2006).
- Knobler S. and others, *The Impact of Globalization on Infectious Disease Emergence and Control: Exploring the Consequences and Opportunities*, (The National Academic Press, 2006).

- Landrain T. and others, 'Do-it-yourself biology: Challenges and Promises for an Open Science and Technology Movement' in *Systems and Synthetic Biology*, (Springer, 2013).
- Langley, C. and Parkinson, S. 'The Political Economy of Military Science', in Tyfield D., Lave R., Randalls S. and Thorpe C., *The Routledge Handbook of the Political Economy of Science*, (Routledge, 2017).
- Leins K., *New war technologies and international law: the legal limits to weaponizing nanomaterials*, (Cambridge University Press, 2022).
- McGraw M. D., 'The story of the Biodiversity Convention: From Negotiation to Implementation', in Le Prestre P.G., *Governing Global Biodiversity: the evolution and implementation of the Convention on Biological Diversity, (*Routledge, 2017).
- Morato-Leite J.R. and others, 'Experience, Mistakes and Challenges: The Implementation of the Convention on Biological Diversity in Brazil' in Jeffery I.M, Firestone J. and Bubna-Litic L., *Biodiversity Conservation, Law and Livelihoods: Bridging the North-South Divide*, (Cambridge University Press, 2008).
- Mortera-Martinez C. 'Game over? Europe's cyber problem', (*Centre for European Reform*, 2018).
- Murray D. and others, *Practitioners' Guide to Human Rights Law in Armed Conflict,* (Oxford University Press, 2016).
- Navas, S., 'Robot Machines and Civil Liability' in Ebers M., and Navas S., *Algorithms and Law*, (Cambridge University Press, 2020).
- Rappert B. and McLeish C., *A Web of Prevention: Biological Weapons, Life Sciences, and the Governance of Research,* (Routledge, 2014).
- Rappert B., 'Can the Law Regulate the Humanitarian Effects of Technologies? ', in Gow J., Dijxhoorn E., Kerr R., Verdirame G., *Routledge Handbook of War, Law and Technology*, (Taylor and Francis, 2019).
- Revill J., Husbands J., and Bowman K., *Governance of Dual Use Research in the Life Sciences: Advancing Global Consensus on Research Oversight*, (The National Academies Press, 2018).
- Ripoll Servent A. 'Protecting or Processing? Recasting EU Data Protection Norms', in Wolf J. Schünemann and Max-Otto Baumann, *Privacy, Data Protection and Cybersecurity in Europe* (Springer 2017).
- Rodríguez-Garavito C., 'A Human Right to a Healthy Environment? ', in Knox J. and Pejan R., *The Human Right to a Healthy Environment* (Cambridge University Press, 2018).
- Ryan J., 'Future Directions for Biosecurity', in *Biosecurity and Bioterrorism*, (2016).
- Rosendal G.K., *The Convention on Biological Diversity and Developing Countries*, (Springer, 2000).

- Salisbury D., 'UNSCR 1540 Implementation: Challenges Past and Present' in Stewart I., Viski A., and Salisbury D., *Preventing the Proliferation of WMDs: Measuring the Success of UN Security Council Resolution 1540,* (Palgrave Macmillan, 2018).
- Segger M-C., Perron-Welch F. and Frison C., *Legal Aspects of Implementing the Cartagena Protocol on Biosafety,* (Cambridge University Press, 2013).
- Sharma A., and others, 'Next generation agents (synthetic agents): Emerging threats and challenges in detection, protection, and decontamination', in S.J.S Flora and Pachauri V., *Handbook on Biological Warfare Preparedness* (*Elsevier*, 2020).
- Schwab K., *The Fourth Industrial Revolution*, (World Economic Forum, 2016).
- Schmitt M., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* (2nd Cambridge University Press, 2017).
- Snowden F., 'The Germ Theory of Disease' in *Epidemics and Society: From the Black Death to the Present*, (Yale University Press, 2019).
- Socher J., *Russia and the Right to Self-Determination in the Post-Soviet Space,* (Oxford University Press, 2021).
- Stearns P., *The Industrial Revolution in World History*, (Routledge, 2020).
- Stewart P., 'Proliferation of Weapons of Mass Destruction', in *Weak Links: Fragile States, Global Threats and International Security,* (Oxford University Press, 2011).
- Susskind R., *The Future of Law: Facing the Challenges of Information Technology,* (Clarendon Press, 1996).
- Tannenwald N., *The Nuclear Taboo,* (Cambridge University Press, 2007).
- Thiele R., *Hybrid Warfare Future and Technologies*, (Springer, 2021).
- Tucker J., *Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies*, (MIT Press, 2012).
- Trump B., Florin M.V., Perkins E. and Linkov I., Biosecurity for Synthetic Biology and Emerging Biotechnologies: Critical Challenges for Governance in Biology' in Trump B, Florin M.V., Perkins E., Linkov I., *Emerging Threats of Synthetic Biology and Biotechnology: Addressing Security and Resilience Issues*, (Springer, 2019).
- Trump D., 'Synthetic Biology, GMO, and Risk: What Is New, and What is Different? ', Trump B.D., Cummings C.L., Kuzma J., Linkov I., *Synthetic biology 2020: frontiers in risk analysis and governance,* (Springer, 2020).
- Tsagourias N., 'The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II—The Use of Force' in Terry D. Gill, *Yearbook of International Humanitarian Law*, (Springer, 2014).

- Tsagourias N., 'Non-State Actors and the Use of Force', in D'Aspremont J., *Participants in the International Legal System: Multiple Perspectives on Non-State Actors in International Law* (Routledge, 2011).
- Verdirame G. and Bencic H. M., 'The Synthetic Biology Dilemma: Dual-use and the limits of academic freedom', in Gow J. and others, *Routledge Handbook of War, Law and Technology*, (Routledge, 2019).
- Ulnicane I., 'The governance of dual-use research in the EU: the case of neuroscience', in Antonio Calcara, Raluca Csernatoni and Chantal Lavallée, *Emerging Security Technologies and EU Governance*, (Routledge, 2020).
- Vamsidhar E., Karthikeyan C., Banerjee D., 'Introduction to the Internet of things', in Prakash K., *Internet of things: from the foundations to the latest frontiers in research*, (De Gruyter, 2021), pp. 1-4.
- Verwey W., 'Observation on the Legal Protection of the Environment in Times of International Armed Conflict' in Kiss A.C. and Lammers J., *Hague Yearbook of International Law*, (Brill, 1994).
- Young M.A., 'Introduction: The Productive Friction between Regimes' in *Regime Interaction in International Law: Facing Fragmentation*, (Cambridge University Press, 2012).
- Young M. A., 'Regime Interaction in Creating, Implementing and Enforcing International Law', in Young M.A., *Regime Interaction in International Law: Facing Fragmentation*, (Cambridge University Press, 2012).
- Young M.A., 'Regime Interaction in Creating, Implementing and Enforcing International Law' in *Regime Interaction in International Law: Facing Fragmentation*, (Cambridge University Press, 2012).
- Wessel R.A., 'Towards EU cybersecurity law: regulating a new policy field', in Tsagourias N., Buchan R. *Research handbook on international law and cyberspace*, (Edward, 2015).
- Zedan H., 'The road to the biosafety protocol', in Le Prestre P.G., *Governing Global Biodiversity: the evolution and implementation of the Convention on Biological Diversity, (*Routledge, 2017).

Journal articles

- Aavitsland P. and others, 'Functioning of the International Health Regulations during the COVID-19 pandemic', (*Lancet*, 2021).
- Abbott K.W and Snidal D., 'Hard and Soft Law in International Governance', (*International Organization*, 2000), 54(3).

- Alheit K., 'The applicability of the EU product liability directive to software', (*Comparative and International Law Journal of Southern Africa*, 2001).
- Al-Khouri A., 'Data Ownership: Who Owns 'My Data'? ', (*International Journal of Management & Information Technology*, 2017), 2(1).
- Amerasinghe, C., 'The Charter Travaux Préparatoires and United Nations Powers to Use Armed Force', (*Canadian Yearbook of International Law*,1966) ', 4.
- Asada M., 'Security Council Resolution 1540 to Combat WMD Terrorism: Effectiveness and Legitimacy in International Legislation', (*Journal of Conflict & Security Law*, 2008), 13(3).
- Atlas R.M. and Dando M., 'The dual-use dilemma for the life sciences: Perspectives, conundrums, and global solutions' (*Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, 2006), 4(3).
- Ayanoğlu F., Elçin A., Murat Elçin Y., 'Bioethical issues in genome editing by CRISPR-Cas9 technology', (*Turkish Journal of Biology*, 2020).
- Bajema, N., DiEuliis, D., Lutes, C., & Lim, Y., 'The Digitization of Biology: Understanding the New Risks and Implications for Governance', (*Center for the Study of Weapons of Mass Destruction*, 2018).
- Barnsby E.R. and Reeves R.S., 'Give Them an Inch, They'll Take a Terabyte: How States May Interpret Tallinn Manual 2.0's International Human Rights Law Chapter', (*Texas Law Review*, 2017).
- Baron R., 'A Critique of the International Cybercrime Treaty', (*Journal of communications law and policy*, 2002), 10(1).
- Barras V., Greub G., 'History of biological warfare and bioterrorism', (*Clinical Microbiology and Infection*, 2014), 20(6).
- Bartolini G., 'The Failure of Core Capacities under the WHO International Health Regulations', (*British Institute of International and Comparative Law*, 2021).
- Baskin C.R., 'Who should be driving US science policy? ', (*Perspectives in Biology and Medicine* ,2019), 62(1).
- Beard J., 'The Shortcomings of Indeterminacy in Arms Control Regimes: The Case of the Biological Weapons Convention', (*The American Journal of International Law*, 2007), 101(2).
- Belo D., War's Future: The Risks and Rewards of Grey Zone Conflict and Hybrid Warfare, (*Canadian Global Affairs Institute*, 2018).
- Bernholz S.A., Bernholz M.J.,Herman G.N., 'Problems of Double Criminality', (*Trial*, 1985), 21(1).

- Blum A. and others, 'Nonstate Actors, Terrorism, and Weapons of Mass Destruction', (*International Studies Review*, 2005), 7(1).
- Boehlke T., and Canfor-Dumas E., 'The Military Contribution to The Prevention of Violent Conflict', (*Security and Peace*, 2017), 35(1).
- Bolsen T., Palm R., and Kingsland J., 'Framing the Origins of COVID-19', (*Science Communication*, 2020), 42(5).
- Bostrom N., 'Information hazards: a typology of potential harms from knowledge', (Review Contemporary Philosophy, 2011).
- Brian Y. and Shui-Yan T., 'From COVID-19 Responses in East Asia: Institutional Infrastructure and Enduring Policy Instruments', (*American Review of Public Administration*, 2020).
- Buchanan A. and Kelley M.C., 'Biodefence and the production of knowledge: rethinking the problem', (*Journal of Medical Ethics*, 2013), 39(4).
- Buchan R., 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? ', (*Journal of Conflict & Security Law*, 2012), 17(2).
- Carrapico, H.; Barrihna, A., 'European Union cyber security as an emerging research and policy field' (*European Politics and Society*, 2018), 19(3).
- Carrapico H. and Barrinha A., 'The EU as a Coherent (Cyber)Security Actor? ', *(Journal of Common Market Studies*, 2017), 55(6).
- Carreras N. and others, 'Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis', (*The Journal of the International Council on Systems Engineering*, 2019), 23(2).
- Cate, F. H., and Mayer-Schonberger, V., 'Tomorrow's privacy. Notice and consent in a world of Big Data', (*International Data Privacy Law*, 2013), 3(2).
- Chandra A. and Idrisova A., 'CBD: A Review of National Challenges and Opportunities for Implementation', (*Biodiversity and Conservation*, 2011), 20(14).
- Christopher F. and Greninger A., 'Biotechnology and Bioterrorism: An unprecedented World', (*Survival*, 2004), 46(2).
- Christou, G., 'The collective securitisation of cyberspace in the European Union', (*West European Politics*, 2019), 42 (2).
- Clough J., 'A World of Difference: The Budapest Convention on Cybercrime and The Challenges of Harmonisation', (*Monash University Law Review*, 2013), 40(3).
- Cogan J., 'Noncompliance and the International Rule of Law', (*The Yale Journal of International Law*, 2006), 31.

- Colin P., 'Debugging the Tallinn Manual 2.0's Application of the Due Diligence Principle to Cyber Operations', (*Washington International Law Association*, 2019), 28(2).
- Cormac R. and Aldrich R., Grey is the new black: covert action and implausible deniability, (*International Affair*s, 2018), 94(3).
- Cosbey A., Burgiel S., 'The Cartagena Protocol on Biosafety: An analysis of results', (*International Institute for Sustainable Development*, 2000).
- Crail P., 'Implementing UN Security Council Resolution 1540: A Risk-Based Approach', (*Nonproliferation Review*, 2006), 13(2).
- Daley J., 'Insecure software is eating the world: promoting cybersecurity in an age of ubiquitous software-embedded systems', (*Stanford Technology Law Review*, 2016), 19(3).
- Daniel Fiott, 'Digitalising Defence: Protecting Europe in the Age of Quantum Computing and the Cloud', (*EUISS Brief*, 2020), 4(2).
- De Beer J. and Jain V., 'Inclusive innovation in biohacker spaces: the role of systems and networks', (*Technology Innovation Management Review*, 2018), 8(2).
- Deborah Katz, 'The Mismatch Between the Biosafety Protocol and the Precautionary Principle', (*Georgetown International Environmental Law Review*, 2000), 13.
- Dembek Z.F., Kortepeter M.G., Pavlin J.A., 'Discernment between deliberate and natural infectious disease outbreaks', (*Epidemiol Infect*, 2007), 135(3).
- Dickinson R., 'The Right to Security - Securing Rights or Securitising Rights', (*Oxford Legal Studies Research Paper*, 2013).
- DiEuliis D., 'Science and Technology: Parsing the Digital Biosecurity Landscape', (*Georgetown Journal of International Affairs*, 2020).
- Diggans J., Leproust E., 'Next steps for access to safe, secure DNA synthesis', (*Frontiers in Bioengineering and Biotechnology*, 2019).
- Dirks E., and Leibold J., 'Genomic Surveillance: Inside China's DNA Dragnet', (*International Cyber Policy Centre*, 2020), 34.
- Dixon T., 'The grey zone of cyber-biological security', (*International Affairs*, 2021), 97(3).
- Djenna A., Harous S., and Eddine Saidouni D., 'Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure', (*Appl. Sci*. 2021), 11(4580).
- Domingo J, 'The Biological Weapons Convention (BWC) And Biosafety Diplomacy', (*Applied Biosafety*, 2008),13(2).
- Dunlap C., 'Lawfare Today: A Perspective', (*Yale Journal of International Affairs*, 2008).
- Dunworth T., Mathews J.R. and McCormack T., 'National Implementation of The Biological Weapons Convention', (*Journal of Conflict & Security Law*, 2006), 11(1).

- Dzedzickis A. and others, 'Advanced Applications of Industrial Robotics: New Trends and Possibilities', (Applied Sciences, 2021), 12(1).
- Edwards B., and others, 'From cases to capacity? A critical reflection on the role of 'ethical dilemmas' in the development of dual-use governance, (*Science and Engineering Ethics*, 2014), 20(2).
- Ehni H.J., 'Dual use and the ethical responsibility of scientists', (*Archivum Immunologiae et Therapiae Experimentalis*, 2008), 56(3).
- Elayyan S. 'The future of education according to the fourth industrial revolution', (*Journal of Educational Technology & Online Learning*, 2021), pp. 4(1).
- Eriksson J. and Giacomello G., 'The Information Revolution, Security, And International Relations: (IR)Relevant Theory?', (*International Political Science Review*, 2006), 27.
- Eriksson D. and others, 'A welcome proposal to amend the GMO legislation of the EU', (*Trends in Biotechnology*, 2018), 36(11).
- Falkner R., 'Regulating Biotech Trade: The Cartagena Protocol on Biosafety', (*International Affairs*, 2000), 76(2).
- Feakes D., 'The Biological Weapons Convention', (*Revue scientifique et technique*, 2017), 36(2).
- Fenwick M., Kaal A. W., Vermeulen E., 'Regulation Tomorrow: What Happens When Technology Is Faster than the Law? ', (*American University Business Law Review*, 2017), 6(3).
- Fidler P.D. and Gostin L., 'The New International Health Regulations: An Historic Development for International Law and Public Health', (*Maurer Faculty*, 2006).
- Fidler D.P., 'From International Sanitary Conventions to Global Health Security: The New International Health Regulations' (*Chinese Journal of International Law*, 2005), 4(2).
- Fidler D. 'Wither the Web? International Law, Cybersecurity and Critical Infrastructure Protection', (*Georgetown Journal of International Affairs*, 2015), 8.
- Fiott D., 'Digitalization and hybrid threats: Assessing the vulnerabilities for European security', (*The European Centre of Excellence for Countering Hybrid Threats*, 2022).
- Fogt M., 'Legal Challenges or "Gaps" by Countering Hybrid Warfare – Building Resilience in Jus Ante Bellum', (*Southwestern Journal of International Law*, 2020).
- Forest J., 'Framework for Analyzing the Future Threat of WMD Terrorism', (*Journal of Strategic Security*, 2012), 5(4).
- Fuchs R.F., 'Academic freedom: its basic philosophy, function, and history', (*Law and Contemporary Problems*, 1963), 28.
- Gahlaut S., 'United Nations Security Council Resolution 1540 Implementation: More of the Same or Brave New World? ', (*Strategic Trade Review*,2019), 5(7).

- Galatas I., 'The misuse and malicious uses of the new biotechnologies', (*Annales des Mines - Réalités industrielles*, 2017).
- George, A. M., 'The National Security Implications of Cyberbiosecurity', (*Frontiers in Bioengineering and Biotechnology*, 2019), 7(51).
- Goldblat J. and Bernauer T., 'Proposals for Strengthening the Biological Weapons Convention', (*Bulletin of Peace Proposals*, 1991), 22(2).
- Goldblat J., 'The Biological Weapons Convention - An overview', (*International Review of the Red Cross*, 1997).
- Goda T., 'The global concentration of wealth', (*Cambridge Journal of Economics*, 2018), 42(1).
- Goding V., Tranter K., 'The machine runs itself: law is technology and Australian embryo and human cloning law', (*Griffith Law Review*, 2021), 30(2).
- Greer S.L., Trump B., 'Regulation and regime: the comparative politics of adaptive regulation in synthetic biology', (*Policy Science*, 2019), 52(4).
- Grosswald L., 'T Cyberattack Attribution Matters Under Article 51 of the U.N. Charter', (*Brooklyn Journal of International Law*, 2011), 36(3).
- Gomez-Tatay L., Hernandez-Andreu J.M., 'Biosafety and biosecurity in synthetic biology: a review', (*Critical Reviews in Environmental Science and Technology*, 2019), 49(17).
- Gostin L.O., Katz R., 'The International Health Regulations: The Governing Framework for Global Health Security', (*Milbank Q*, 2016).
- Gostin L.O., 'Pandemic influenza: public health preparedness for the next global health emergency', (*Law, Medicine and Ethics*, 2004).
- Gronvall G., Biosecurity: the opportunities and threats of industrialization and personalization, (*Bulletin of the Atomic Scientists*, 2015), 71(6).
- Haider N., and other, 'Covid-19 – Zoonosis or Emerging Infectious Disease? ', (*Frontiers in Public Health*, 2020), 8.
- Haradhan M., 'Third Industrial Revolution Brings Global Development', (*Journal of Social Sciences and Humanities*, 2021), 7(4).
- Haradhan M., 'The First Industrial Revolution: Creation of a New Global Human Era', (*Journal of Social Sciences and Humanities*, 2019), 5(4).
- Harris R.C., 'State Responses to Biotechnology: Legislative Action and Policymaking in the U.S., 1990–2010', (*Politics and the Life Sciences*, 2015), 34(1).
- Hertogen A., 'Letting Lotus Bloom', (*The European Journal of International Law*, 2016), 26(4).
- Hindmarsh R. and Gottweis, 'Recombinant regulation: The Asilomar legacy 30 years on'. (*Science as Culture*, 2006), 14(4).

- Hoffman F., 'Conflict in the 21st Century: The Rise of Hybrid Wars', (*Potomac Institute for Policy Studies*, 2007).
- Huigang L. and others, 'Development of and prospects for the biological weapons convention', (*Journal of Biosafety and Biosecurity*, 2022), 4(1).
- Ienca M., Effy V., 'Dual use in the 21st century: emerging risks and global governance', (*Swiss Medical Review*, 2018).
- Ienca M., Jotterand, F. and Elger, B.S., 'From Healthcare to Warfare and Reverse: How Should We Regulate Dual-Use Neurotechnology?', (*Neuron*, 2018), 97.
- 'International Humanitarian Law and the Targeting of Data', (*International Law Studies*, 2018), 94.
- James K. Wither, 'Defining Hybrid Warfare', (*Journal of European Security Defense*, 2020), 10(1).
- Javaid M., Haleem A., Singh R., Suman R., 'Substantial capabilities of robotics in enhancing industry 4.0 implementation', (*Cognitive Robotics*, 2021), 1.
- Jiang S., and others, 'Environment and food safety: a novel integrative review', (*Environmental Science and Pollution Research*, 2021), 28.
- Kasper, A., Osula, A. and Molnár, A., 'EU cybersecurity and cyber diplomacy. (*IDP Revista de Internet Derecho y Política*', 2021), 34.
- Katz R., and Fischer J., 'The Revised International Health Regulations: A Framework for Global Pandemic Response', (*Global Health Governance*, 2010), 3(2).
- Kedgley L.A., 'Is it Better to Be Safe than Sorry? The Cartagena Protocol Versus the World Trade Organisation', (*Victoria University of Wellington Law Review*, 2005), 36(2).
- Kelley M., 'Challenges to Compliance with International Humanitarian Law in the Context of Contemporary Warfare', (*Independent Study Project*, 2013).
- Kemp L. and others, 'Bioengineering Horizon Scan 2020', (*eLife*, 2020), 9.
- Kempner J., Merz J.F. and Bosk C.L., 'Forbidden knowledge: public controversy and the production of nonknowledge', (*Sociological Forum*, 2011), 26(3).
- King W., and Guillemin J., 'The price of alliance: Anglo-American intelligence cooperation and Imperial Japan's criminal biological warfare programme, 1944–1947', (*Intelligence and National Security*, 2018), 34(2).
- Kluge H. and others, 'Strengthening global health security by embedding the International Health Regulations requirements into national health system', (*BMJ Global Health*, 2018).
- Knight D., 'COVID-19 Pandemic Origins: Bioweapons and the History of Laboratory Leaks', (*Southern Medical Journal*, 2021), 114(8).

- Koblentz G., 'Pathogens as Weapons: The International Security Implications of Biological Warfare', (*International Security*, 2004), 28(3).
- Koh N.S., Ituarte-Lima C. and Hahn T., 'Mind the Compliance Gap: How Insights from International Human Rights Mechanisms Can Help to Implement the Convention on Biological Diversity', (*Transnational Environmental Law*, 2022), 11(1).
- Kosal M., 'Emerging Life Sciences and Possible Threats to International Security', (Orbis, 2020), 64(4).
- Krink N., Löchner A., Cooper H., Beisel, C. and Di Ventura B., 'Synthetic biology landscape and community in Germany', (*Biotechnology Notes*, 2022), 3.
- Krueger A., 'An enduring need: multilateralism in the twenty-first century', (*Oxford Review of Economic Policy*, 2007), 23(3).
- Kuhlau F. and others, 'A precautionary principle for dual-use research in the life sciences', (*Bioethics*, 2011), 25(1).
- Kumari S., Goel H., 'Exploring the Architecture of Fourth Industrial Revolution: Globalization 4.0', (*Journal of International Business*, 2020), 7(2).
- Lawson G., 'Negotiated revolutions: the prospects for radical change in contemporary world politics', (Review of international studies, 2005), 31(3).
- Lee J. 'IHR 2005 in the Coronavirus Pandemic: A Need for a New Instrument to Overcome Fragmentation? ', (*Asil insights*, 2000), 26(16).
- Le Prestre P.G., 'The CBD at Ten: The Long Road to Effectiveness', (*Journal of International Wildlife Law and Policy*, 2002), 5(3).
- Li J. and others, 'Advances in Synthetic Biology and Biosafety Governance', (*Frontiers in Bioengineering and Biotechnology*, 2021), 9.
- Luukas K. Ilves and others, 'European Union and NATO Global Cybersecurity Challenges: A Way Forward', (*Institute for National Strategic Security*, 2016), 6(2).
- Mandl K.D., Overhage J.M., 'Wagner M.M., and others, 'Implementing syndromic surveillance: a practical guide informed by the early experience', (*Journal of American Medical Informatics Association*, 2004).
- Mansour S.L., Thomas K.R., Capecchi M.R., 'Disruption of the proto-oncogene int-2 in mouse embryo-derived stem cells: a general strategy for targeting mutations to non-selectable genes', (*Nature*, 1988).
- Marks S., 'State-Centrism, International Law, and the Anxieties of Influence', (*Leiden Journal of International Law*, 2006).

- McGraw D., 'The CBD: Key Characteristics and Implications for Implementation', (*Reciel*, 2022),11(1).
- McHugan A., 'Problems with the Cartagena Protocol', (*Asia Biotechnology*, 2006), 10(12).
- Meier O., 'Verification of the biological weapons convention: What is needed? ', (Medicine, Conflict and Survival, 2002), 18(2).
- Miller S., Selgelid M., 'Ethical and Philosophical Consideration of the Dual-use Dilemma in the Biological Sciences', (*Science and Engineering Ethics*, 2007), 13.
- Mills, I., 'Emergent International Humanitarian Law in the Context of Cyber Warfare', (*Journal of Film and Media Studies, 2017)*, 2(1).
- Miquelon-Weismann M., 'The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process? ',(*John Marshall Journal of Computer and Information Law*, 2005), 23(2).
- Morgera, E., 'Dawn of a New Day? The Evolving Relationship between the Convention on Biological Diversity and International Human Rights Law', (*Wake Forest Law Review*, 2018).
- Mueller S., 'Facing the 2020 Pandemic: What Does Cyberbiosecurity Want Us to Know to Safeguard the Future? ' (*Biosafety and Health*, 2020).
- Murch R. and others, 'Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy' (*Frontiers in Bioengineering and Biotechnology*, 2018), 6(39).
- Ndi G., 'International Regulation of Armed Conflicts: 'Jus in Bello' in an Age of Increasingly Asymmetric and Hybrid Warfare', (*Journal of Law and Social Sciences*, 2018), 7(1).
- Nelson M., Roffey P., 'McNevin D., Lennard C., Gahan M.E., 'An overview of biosecurity in Australia', (*Australian Journal of Forensic Sciences*, 2014), 46(4).
- O' Birkeland J., 'The Concept of Autonomy and the Changing Character of War', (*Oslo Law Review*, 2018), 5(2).
- O'Brien J. and Nelson C., 'Assessing the Risks Posed by the Convergence of Artificial Intelligence and Biotechnology', (*Health Security*, 2020), 18(3).
- Oltmann, S., 'Dual-Use Research: Investigation Across Multiple Science Disciplines', (*Science and Engineering Ethics*, 2015), 21.
- Ostergard R., Tubin M., and Altman J., 'Stealing from the past: globalization, strategic formation and the use of indigenous intellectual property in the biotechnology industry', (*Third World Quarterly*, 2001), 22(4).
- Park H., 'Technology convergence, open innovation, and dynamic economy', (*Journal of Open Innovation: Technology, Market, and Complexity*, 2017), 3(24).

- Peccoud J, and others, 'Cyberbiosecurity: From Naive Trust to Risk Awareness', (*Trends in Biotechnology*, 2018), 36(1).
- Pert A., 'International Law in a Post-Post-Cold War World—Can It Survive? ', (*Asia and the Pacific Policy Studies*, 2017), 4(2).
- Pilloud C., 'Reservations to the Geneva Conventions of 1949', (*International Review of the Red Cross*, 1976).
- Porcedda M.G., 'Patching the patchwork: appraising the EU regulatory framework on cyber security breaches', (*Computer Law and Security Review*, 2018), 34(5).
- Premanandh J., 'Global consensus –Need of the hour for genetically modified organisms (GMO) labeling', (*Journal of Commercial Biotechnology*, 2011), 17 (1).
- Qin W., Chen S., Peng M., 'Recent advances in Industrial Internet: insights and challenges', (*Digital Communications and Networks*, 2020), 6(1).
- Rajagopal B., 'Academic freedom as a human right: An internationalist perspective', (*Journal of the American Association of University Professors*, 2003), 89(3).
- Rappert B., 'Why Has Not There Been More Research of Concern?, (*Frontiers in Public Health*, 2014).
- Reed J. and Dunaway N., 'Cyberbiosecurity Implications for the Laboratory of The Future', (Frontiers in Bioengineering and Biotechnology, 2017), 7(182).
- Rehman H. and Qazi A., 'Significance of UNSCR 1540 and Emerging Challenges to its Effectiveness', (*Strategic Studies*, 2019), 39(2).
- Riordan, S., 'The Geopolitics of Cyberspace: A Diplomatic Perspective', (*Brill Research Perspectives in Diplomacy and Foreign Policy*, 2018), 3(3).
- Rychnovská D., 'Governing dual-use knowledge: From the politics of responsible science to the ethicalization of security', (*Security Dialogue*, 2016), 47(4).
- Roberts K., 'New Challenges in Organisational Research: High Reliability Organisations', (*Industrial Crisis Quarterly*,1989), 3(2).
- Roberts G., 'The New Rules for Waging War: The Case against Ratification of Additional Protocol', (*Virginia Journal of International Law*, 1985).
- Rodrigues R., 'Legal and human rights issues of AI: Gaps, challenges and vulnerabilities', (*Journal of Responsible Technology*, 2020), 4.
- Rohden F., 'Proceedings of the Dual Use Research of Concern Panel Discussion: challenges and perspectives', (*Canadian Journal of Microbiology*, 2022).
- Rosenstock L. and Lee L.J., 'Attacks on Science: The Risks to Evidence-Based Policy', (*Ethics and Public Health*, 2002).

- Salloch S. 'The dual use of research ethics committees: why professional self-governance falls short in preserving biosecurity', (*BMC Medical Ethics*, 2018).
- Sari A., 'Hybrid threats and the law: Concepts, trends and implications', (*The European Centre of Excellence for Countering Hybrid Threats*, 2020).
- Schiemann J., 'The OECD Blue Book on Recombinant DNA Safety Considerations: it's influence on ISBR and EFSA activities', (*Environmental Biosafety Research*. 2006).
- Schmitt M., 'Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance', (*Virginia Journal of International Law*, 2010).
- Schmitt M. and Watts S., 'Beyond State-Centrism: International Law and Non-state Actors in Cyberspace', (*Journal of Conflict & Security Law*, 2016), 21(3).
- Schmitt M., 'Green War: An Assessment of the Environmental Law of International Armed Conflict', (*Yale Journal of International Law*, 1997), 22(1).
- Schermer, B. W., Custers, B., and Van Der Hof, S., 'The crisis of consent: How stronger legal protection may lead to weaker consent in data protection', (*Ethics and Information Technology*, 2014), 2.
- Schneier B, 'Securing Medical Research: A Cybersecurity Point of View', (*Science*, 2012), 336(6088).
- Schneider J., 'The BWC's Prohibition of Biological Weapons: Reality or Rhetoric? ', (*Journal of Biosecurity, Biosafety, and Biodefense Law*, 2014).
- Schoiswohl M., 'Human Rights and Disarmament – A Blind Date or Shotgun Marriage? ', (*Austrian Review of International and European Law*, 2013), 15(1).
- Selgelid, M.J., 'Dual-Use Research Codes of Conduct: Lessons from the Life Sciences', (*Nanoethics*, 2009).
- Selgelid M.J., 'Gain-of-function research: ethical analysis', (*Science and Engineering Ethics*, 2016), 22(4).
- Singh P. and Jairath G., and Ahlawat S., 'Nanotechnology: a future tool to improve quality and safety in meat industry', (*Journal of Food Science and Technology*, 2016), 53(4).
- Sjöstedt B. and Dienelt A., 'Enhancing the Protection of the Environment in Relation to Armed Conflicts: Draft Principles of the International Law Commission and beyond', (*Goettingen Journal of International Law*, 2020).
- Smith J.A. and Sandbrink J.B., 'Biosecurity in an age of open science', (*Plos Biology*, 2022), 20(4).
- Snape J. W., 'Joining the Convention on Biological Diversity: A Legal and Scientific Overview of Why the United States Must Wake Up ', (*Sustainable Development Law & Policy*, 2010), 10(3).

- Sohn M., Ro D. and others, 'The problems of International Health Regulations (IHR) in the process of responding to COVID-19 and improvement measures to improve its effectiveness', (*Journal of Global Health Science*, 2021), 3(2).
- Sohrabi C., 'World Health Organization declares global emergency: A review of the 2019 novel coronavirus' (COVID-19), (*International Journal of Surgery*, 2020), 76.
- Spicer N., Agyepong I., Ottersen T., Jahn A., Ooms G., 'It's far too complicated': why fragmentation persists in global health', (*Global Health*, 2020), 16(1).
- Stanzel V. and others, 'New Realities in Foreign Affairs: Diplomacy in the 21st Century', (*SWP*, 2018), 11.
- Stern J., 'Dreaded Risks and the Control of Biological Weapons', (*International Security*, 2002), 27(3).
- Stewart D., 'New Technology and the Law of Armed Conflict', (*International Law Studies*, 2011).
- Stokes D., 'Trump, American Hegemony and the Future of the Liberal International Order', (*International Affairs*, 2018), 94(1).
- Sture J., Whitby S. and Perkins D., 'Biosafety, biosecurity and internationally mandated regulatory regimes: compliance mechanisms for education and global health security', (*Medicine, Conflict and Survival*, 2013).
- Sturtevant J.L., Anema A. and Brownstein J.S., 'The new International Health Regulations: considerations for global public health surveillance', (*Disaster Medicine and Public Health Preparedness*, 2007).
- Suk J.E., Bartels C., Broberg E., Struelens M.J., Ozin A.J., 'Dual-use research debates and public health: better integration would do no harm', (*Frontiers in Public Health*, 2014).
- Talbot Jensen E., 'The Tallinn Manual 2.0: Highlights and Insights', (*Georgetown Journal of International Law*, 2017).
- Taylor A. and Habibi R., 'The Collapse of Global Cooperation under the WHO International Health Regulations at the Outset of COVID-19: Sculpting the Future of Global Health Governance', (*American Society of international Law*, 2020), 24(15).
- Thimbleby H., 'Technology and the Future of Healthcare', (*Journal of Public Health Research*, 2013), 2(3).
- Thomas M. Franck, 'Terrorism and the Right of Self-Defense' (*American Journal of International Law*, 2001), 95.
- Tinker C., 'A "New Breed" of Treaty: The United Nations Convention on Biological Diversity', (*Pace Environmental Law Review*, 1995), 13(1).

- Trump B.D., 'Synthetic biology regulation and governance: lessons from TAPIC for the United States, European Union, and Singapore', (*Health Policy*, 2017), 121(11).
- Ulven J.B., Wangen G., 'A Systematic Review of Cybersecurity Risks in Higher Education', (*Future Internet*. 202), 13(2).
- Upeniece, V., 'Conditions for the lawful exercise of the right of self-defence in international law', (*SHS Web of Conferences*, 2018).
- Valenduc G. and Vendramin P., 'Digitalisation, between Disruption and Evolution', (*European Review of Labour and Research*, 2017), 23(2).
- Van Der Vossen B., 'The Asymmetry of Legitimacy', (*Law and Philosophy*, 2012), 31(5).
- Van Deveer S.D. and Dabelko G.D., 'It's Capacity, Stupid: International Assistance and National Implementation', (*Global Environmental Politics*, 2001).
- Vennis M.I. and others, 'Complementarity of International Instruments in the Field of Biosecurity', (*Policy and Practice Reviews*, 2022).
- Vinke S., Rais I., and Millett P., 'The Dual-Use Education Gap: Awareness and Education of Life Science Researchers on Nonpathogen-Related Dual-Use Research', (*Health Security*, 2022), 20(1).
- Vrielinka J. and others, 'Academic Freedom as a Fundamental Right', (*Procedia Social and Behavioral Sciences*, 2011).
- Walsh P.F., 'The Biosecurity Threat Environment', (*Intelligence, Biosecurity and Bioterrorism*, 2018).
- Weisdorf J., 'From Foraging to Farming: Explaining the Neolithic Revolution', (*Journal of Economic Surveys*, 2005), 19(4).
- Wilson, K., Halabi, S. and Gostin, L.O. 'The International Health Regulations (2005), the threat of populism and the COVID-19 pandemic', (*Global Health*, 2020), 16(70).
- Wintle B. and others, 'A Transatlantic Perspective on 20 Emerging Issues in Biological Engineering' (*eLife*, 2017), 6.
- Wright J., Avouris A., Frost M. and Hoffmann S., 'Supporting academic freedom as a human right: challenges and solutions in academic publishing', (*The International Journal of Human Rights*, 2022).
- Yen-Hsiang W. and others, 'Synthetic biology: advancing the design of diverse genetic systems', (*Annual Review of Chemical and Biomolecular Engineering*, 2013).
- Yim Guo R. D., 'Ethical Theory for Dual-Use Dilemmas in Synthetic Biology', (*Asian Bioethics Review*, 2012), 4(2).
- Youngrim K., Chen Y., 'Liang F., Engineering care in pandemic technogovernance: The politics of care in China and South Korea's COVID-19 tracking apps', (*New Media and Society*, 2017).

- Yuying Liu I., 'The due Diligence Doctrine under Tallinn Manual 2.0', (*Computer Law & Security Review*, 2017), 33(3).
- Zidar A., 'WHO International Health Regulations and Human Rights: From Allusions to Inclusion', (*British Institute of International and Comparative Law*, 2015.

Conventions

- Council of Europe, 'Convention for the Protection of Human Rights and Fundamental Freedoms', Rome, (1950), ETS 5, entry into force 3 September 1953.
- Council of Europe, 'European Convention on Mutual Assistance in Criminal Matters', Strasbourg, (1959), ETS 30, entry into force 12 June 1962.
- Council of Europe, 'Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence', Strasbourg, (2022), ETS 185.
- Council of Europe, 'European Convention for the Protection of Human Rights and Fundamental Freedoms', as amended by Protocols Nos. 11 and 14, Rome (1950), ETS 55, entry into force 3 September 1953.
- Council of Europe, 'Convention on Cybercrime', Budapest, (2000), ETS 185, entry in force 1 July 2004
- Council of Europe, 'Convention on Cybercrime', Budapest, (2000), ETS 185, entry in force 1 July 2004.
- Council of Europe, 'European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14', Rome, (1950), ETS 55, entry into force 20 December 1971.
- International Committee of the Red Cross (ICRC), 'The Hague Conventions of 1899 (II): Respecting the Laws and Customs of War on Land', Hague, (1915), entry into force 9 September 1900.
- International Committee of the Red Cross (ICRC), 'Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)', Geneva, (1978), entry into force 7 December 1979.
- International Peace Conferences, 'Hague Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land', The Hague, (1907), entry into force 26 January 1910.
- Organization of African Unity (OAU), 'African Charter on Human and Peoples' Rights', Banjul, (1981), CAB/LEG/67/3 rev. 5, 21 I.L.M. 58, entry into force 21 October 1986.

- Organization of American States (OAS), 'American Convention on Human Rights', Costa Rica, (1969), 1144 UNTS 123, entry into force 18 July 1978.
- The World Conservation Union, 'Convention on International Trade in Endangered Species of Wild Fauna and Flora', Washington D.C., (1973), 993 UNTS 243, entry into force 1 July 1975.
- UN General Assembly, 'United Nations Framework Convention on Climate Change', New York, (1992), Rio de Janeiro, 1992, entry into force 21 March 1994, A/RES/48/189.
- UN General Assembly, International Covenant on Civil and Political Rights, New York, (1966), 999 UNTS 171, entry into force 23 March 1976.
- UN General Assembly, 'United Nations Convention against Transnational Organized Crime: resolution / adopted by the General Assembly', (2001), A/RES/55/25.
- United Nations, 'Charter of the United Nations', San Francisco, (1945), 1 UNTS XVI, entry into force 14 October 1945.
- United Nations, 'Cartagena Protocol on Biosafety to the Convention on Biological Diversity', Montreal, (2000), 2226 UNTS 208, entry into force 11 September 2003.
- United Nations, 'Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects', Geneva (1980), 1342 UNTS 137, entry into force 2 December 1983.
- United Nations, General Assembly, 'International Covenant on Economic, Social, and Cultural Rights', New York, (1966), 993 UNTS 3, entry into force 3 January 1976.
- United Nations, 'Convention of the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction', New York, (1971), 1015 UNTS, entry into force 26 March 1975.
- United Nations, 'Convention on Biological Diversity', Rio de Janeiro, (1992), Nairobi, 1992, entry into force 29 December 1993, 1760 UNTS 79, 31 ILM 818.
- United Nations, 'Vienna Convention on the Law of Treaties', Vienna, (1969), 1155 UNTS 331, entry into force 27 January 1980.
- United Nations Educational, Scientific and Cultural Organization, 'Convention on wetlands of international importance especially as waterfowl habitat', Ramsar, (1971), 996 UNTS 245, entry into force 21 December 1975.

UN documents

- UN Security Council, 'Security Council resolution 1540', (2004), S/RES/1540.
- UN Security Council, 'Security Council resolution 1673', (2006), S/RES/1673.
- UN Security Council, 'Security Council resolution 418', (1977), S/RES/418.

- UN Security Council, 'Security Council resolution 2325', (2016), S/RES/2325.
- UN Security Council, 'Security Council resolution 1540', (2004), S/RES/1540.
- UN Security Council, 'Security Council resolution 1566', (2004), S/RES/1566.

Other international legal instruments

- International Law Commission, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts', (2001), Supplement No. 10 (A/56/10), chp.IV.E.1.
- Marrakesh Agreement Establishing the World Trade Organization, Marrakesh (1994), 1867 U.N.T.S. 154, 33 I.L.M. 1144, entry into force 1 January 1995.
- United Nations, 'Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or other Gases, and of Bacteriological Methods of Warfare', Geneva, (1925), entry into force 8 February 1928.
- World Health Organization, 'International Health Regulations', Geneva, (2005), 2509 UNTS 79, entry into force 15 June 2007.
- World Health Assembly, 'Revision and Updating of the International Health Regulations', Geneva, (1995), WHA48.7.
- World Health Assembly, 'Revision of the International Health Regulations', Geneva, (2003), WHA56.28.
- UN General Assembly, 'Universal Declaration of Human Rights', New York, (1948), 217 A (III).
- UN General Assembly, 'International Covenant on Civil and Political Rights', 16 December 1966, UNTS 999, 16 December 1966, New York, entry into force 23 March 1976.

EU Legislation

- European Commission, 'Revised Directive on Security of Network and Information Systems (NIS2)', Brussels, 2020.
- The Council of the European Union, 'Council Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States', Brussels, (2019).
- The Council of the European Union, 'Council Regulation (EU) 2020/2094 of 14 December 2020 establishing a European Union Recovery Instrument to support the recovery in the aftermath of the COVID-19 crisis', Brussels, (2020).
- The Council of the European Union, 'Council Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States', Brussels, (2019).

- The Council of the European Union, 'Council Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States', Brussels, (2019).
- The Council of the European Union, 'Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products', (1985).
- The European Parliament and the Council, 'Proposal for a Directive on the resilience of critical entities', Brussels, (2020).
- The European Parliament and the Council of the European Union, 'Regulation (EU) 2019/881 of the European Parliament and of the Council of 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', Brussels, (2019).
- The European Parliament and the Council of the European Union, 'Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union', Brussels, (2016).
- The European Parliament and the Council of the European Union, 'Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union', Brussels, (2016), Annex II.
- The European Parliament and the Council of the European Union, 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data', Brussels, (1995).
- The European Parliament and the Council of the European Union, 'Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union', Brussels, (2016).
- The European Parliament and the Council, 'Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148', Brussels, (2020).
- The European Parliament and the Council of the European Union, 'Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC', Brussels, (2016).
- The European Parliament and the Council of the European Union, 'Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC', Brussels, (2016).

International Case Law

- International Court of Justice (ICJ), *'Case Concerning Military and Paramilitary Activities in and against Nicaragua*' (Nicaragua v. United States of America), 1986.
- Court of Justice of the European Union (CJEU), *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, CJEU - C-311/18, (2018).

Miscellaneous

- Assumpção C., 'The Problem of Cyber Attribution Between States', (*E- International Relations*, 2020).
- Bendiek A. and Schulze M., 'Attribution: A Major Challenge for EU Cyber Sanctions an Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW' (*SWP*, 2021), 11.
- Bendiek, A., 'European Cyber Security Policy', (SWP 2012), 13.
- Bertschek I., and others, 'The Economic Impacts of Telecommunications Networks and Broadband Internet', (*Center for European Economic Research*, 2016).
- Bipartisan Commission on Biodefence, 'Cyberbio Convergence: Characterizing the Multiplicative Threat', Washington, (2019); Available at: <https://biodefensecommission.org/events/cyberbio-convergence-characterizing-the-multiplicative-threat/>, (accessed 22 May 2022).
- Buccina J., Dylan G. Weber A., 'Biological Deterrence for The Shadow War', (*Texas National Security Review*, 2021).
- Cameron E., Nuzzo J. and Bell. J., 'Global Health Security Index: Building Collective Action and Accountability', (*Center for Health Security*, 2019).
- Council of Europe, 'Explanatory Report to the Convention on Cybercrime', Budapest, (2001), ETS 185.
- Carus W., 'A Short History of Biological Warfare: From Pre-History to the 21st Century', (*Center for the Study of Weapons of Mass Destruction*, 2017).
- Cebo D., 'Strategical Analysis of Cyberbiosecurity in 2022: How to Defend Biotech and Healthcare Sector from Cyber Treats', (2022).
- Cong W., 'Seeking Customary International Human Rights Law in the Cyberspace: A Critique of the Tallinn Manual 2.0', (2018), Available at SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3744924>, (accessed 9 July 2022).
- Constant P., 'Guardian of the Galaxy? Assessing the European Union's International Actorness in Cyberspace', (*College of Europe*, 2021).

- Christou, G. Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy, (New Security Challenges Series 2016).
- Cruickshank P., and Rassler D., 'A Virtual Roundtable on COVID-19 and Counterterrorism' (CTL Sentinel, 2020), 13(6).
- CSIS, 'The Biological Weapons Threat and Nonproliferation Options: A Survey of Senior U.S. Decision Makers and Policy Shapers', (*CSIS*,2006).
- Diamond E., 'Applying International Humanitarian Law to Cyber Warfare', (*Institute for National Security Studies*, 2014).
- Dickinson R., 'The Right to Security - Securing Rights or Securitising Rights', (*Oxford Legal Studies Research Paper*, 2013).
- ENISA, 'Definition of cybersecurity: gaps and overlaps in standardization', (2016), pp. 10-12.
- Erskine S., 'The EU Tiptoes into Cyber Sanctions Regimes', (*RUSI*, 2020).
- European Commission and HREU, 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', (2013).
- European Commission, 'Proposal for a directive of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM/2012/010 final', (2012,a).
- European Commission, 'Rolling Plan for ICT Standardisation 2021', Brussels, (2021).
- European Commission, 'Communication: A Digital Single Market Strategy for Europe', Brussels, (2015).
- 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 on the EU Security Union Strategy', Brussels, (2020).
- European Commission, 'Commission Staff Working Document, Impact assessment accompanying the document proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification', (2017).
- European Union, 'Consolidated version of the Treaty on the Functioning of the European Union', (2008), entry into force 1 December 2009.
- European Commission, 'Joint Communication Resilience, Deterrence and Defence: Building strong cybersecurity for the EU', Brussels, (2017).

- European Court of Auditors, 'Challenges to effective EU cybersecurity policy', (2019), pp. 33-39, Available at: <https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf>, (accessed 27 May 2022).
- European Digital Rights, 'Ratification by EU Member States of the Second Additional Protocol of the Council of Europe Cybercrime. Convention Why is the opinion of the Court of Justice of the European Union necessary? ', (*EDRi*, 2022).
- European Defence Agency, 'EDA Technology Foresight Exercise 2021: Welcome to the Futures – Future Narratives', (2021), Available at: <https://eda.europa.eu/docs/default-source/documents/202105-edatechnologyforesightexercise-futuresnarratives_v5.pdf>, (accessed 12 July 2022).
- Fantin S. 'Weighting the EU Cybersecurity Act: Progress or Missed Opportunity? ', (*CiTiP, KU Leuven Centre for IT & IP Law*, 2019), Available at: < https://www.law.kuleuven.be/citip/blog/weighting-the-eu-cybersecurity-act-progress-or-missed-opportunity/ >, (accessed 23 May 2022).
- Frinking E. and others, 'The Increasing Threat of Biological Weapons: Handle with Sufficient and Proportionate Care', (*The Hague Centre for Strategic Studies*, 2016).
- Galates I., 'The Misuse and Malicious Uses of the New Biotechnologies', (*Cairn*, 2017), pp. 103.
- General Secretariat of the Council, 'EU Cyber Defence Policy', 14413/18, Brussels, (2018).
- Giannopoulos G., Smith H., and Theocharidou M., 'The Landscape of Hybrid Threats: A Conceptual Model Public Version', (*European Commission*, 2021).
- Gillam M. M., 'Information Warfare: Combating the Threat in the 21st century', (1997).
- Global Civil Society, 'Submission to the Council of Europe, Comments and suggestions on the Terms of Reference for drafting a Second Optional Protocol to the Cybercrime Convention', (2017), Available at: <https://edri.org/files/surveillance/cybercrime_2ndprotocol_globalsubmission_e-evidence_20170908.pdf>, (accessed 14 May 2022).
- Government of Malaysia, 'Fifth National Report to the CBD', (2014), p. 90, Available at: <https://www.cbd.int/doc/world/ my/my-nr-05-en.pdf>, (accessed 7 June 2022).
- Healey J., 'Beyond Attribution: Seeking National Responsibility for Cyberattacks', (*Atlantic Council*, 2012).
- High Representative of the Union for Foreign Affairs and Security Policy, Vice-President of the European Commission, and Head of the European Defence Agency, 'Implementation Plan on Security and Defence', 14392/16, Brussels, (2016).

- Hoffman W. and Levite A., 'Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?' (*Carnegie*, 2017).
- Hutchins G. S. Pirolli L. P. and K. Card K.S., 'What Makes Intelligence Analysis Difficult? A Cognitive Task Analysis of Intelligence Analysts', (*Calhoun*, 2007).
- ICRC, New technologies and warfare, (*International Review of the Red Cross*, 2012), 94(886).
- International Committee of the Red Cross, 'Functional Perspective on the Biological Weapons Convention and Chemical Weapons Convention', (2006), Available at: <https://www.icrc.org/en/doc/resources/documents/statement/biological-chemical-weapons-statement-111206.htm>, (accessed 20 July 2022).
- International Crisis Group, 'The Politics Behind the Ebola Crisis', Africa Report n° 232, (2015).
- Interpol, 'Bioterrorism Incident Pre-planning and response guide', (2007).
- Interpol, 'Cybercrime: Covid-19 Impact', (2020).
- ICJ, 'Legality of the Threat or Use of Nuclear Weapons', Advisory Opinion, July 8, 1996, ICJ Rep. 1996.
- Lentzos F., 'Compliance and Enforcement in the Biological Weapons Regime', (*United Nations Institute for Disarmament Research*, 2019).
- Levite A, Chuanying L. Perkovich G. and Yang F., 'Managing U.S.-China Tensions Over Public Cyber Attribution', (*Carnegie*, 2022).
- Kasapoglu C., 'Cyber Security: Understanding the Fifth Domain', (Centre for Economics and Foreign Policy Studies, 2017).
- Kavanagh C., 'New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses? ', (*Carnegie*, 2019).
- Klimburg A. and Faesen L., 'A balance of Power in Cyberspace', (*The Hague Centre for Strategic Studies*, 2022).
- Knox, J.H., 'Report of the Special Rapporteur on the Issue of Human Rights Obligations Relating to the Enjoyment of a Safe, Clean, Healthy and Sustainable Environment', (*Knox Biodiversity Report*, 2017).
- McDevitt M., and others, 'The Changing Nature of Warfare', (*Center for Strategic Studies*, 2004).
- Michael J. Ainscough, 'Next Generation Bioweapons', (*USAF Counterproliferation Center*, 2002).
- Ministry of Environment, Forest and Climate Change, Government of India, 'Voluntary Peer-Review under the Convention on Biological Diversity. Case Study 2: India', Available at: <https://www.cbd.int/doc/nbsap/in-vpr-en.pdf>, (accessed 7 June 2022).
- Morris L. and others, *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*, (Rand Corporation, 2019).

- Mulligan S., 'Withdrawal from International Agreements: Legal Framework, the Paris Agreement, and the Iran Nuclear Agreement', (*Congressional Research Service*, 2018), Available at: < https://sgp.fas.org/crs/row/R44761.pdf>, (accessed on 16 July 2022).
- National Research Council, 'Biotechnology Research in an Age of Terrorism: Confronting the Dual Use Dilemma', (*National Academy Press*, 2004).
- National Science Advisory Board for Biosecurity, 'National Science Advisory Board for Biosecurity Charter', (2004).
- NATO Science & Technology Organization, 'Science & Technology Trends: 2020-2040 – Exploring the S&T Edge', March 2020, Available at: <https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf>, (accessed 11 July 2022).
- Nelli Feroci F., Greco E. and Pirozzi N., 'Renewing Multilateralism for the 21st century: the Role of the United Nations and of the European Union', (*IAI*, 2020).
- Organization for Economic Co-operation and Development, 'Recombinant DNA Safety Considerations - Safety considerations for industrial, agricultural and environmental applications of organisms derived by recombinant DNA techniques', (1986), Available at: <https://bch.cbd.int/en/database/48487>, (accessed 4 June 2022).
- Pauwels E., 'The New Geopolitics of Converging Risks: The UN and Prevention in the Era of AI' (*United Nations University Centre for Policy Research*, 2019).
- Pauwel E., 'Cyber-biosecurity: How to protect biotechnology from adversarial AI attacks', (Hybrid CoE, 2021).
- Pomeroy R.., 'Ransomware And 'Ransom-War': Why we must be Ready for Cyberattacks' (*World Economic Forum*, 2022).
- Reichart J.F. and Caves, J., 'The Future of Weapons of Mass Destruction: their Nature and Role in 2030', (*Center for the Study of Weapons of Mass Destruction*, 2014).
- Republic of South Africa, 'Fifth National Report to the CBD', Mar. 2014, Available at: <https://www.cbd.int/doc/world/za/za-nr-05-en.pdf>, (accessed 7 June 2022).

Republic of South Sudan, 'Fifth National Report to the CBD', (2015), Available at: <https://www.cbd.int/doc/world/ss/ss-nr-05-en.pdf>, (accessed 7 June 2022).

- Sánchez V. and Juma C., *Biodiplomacy: Genetic Resources and International Relations*, (African Centre for Technology Studies, 1994).
- Sandage J. et al., 'Comprehensive Study on Cybercrime', (United Nations Office on Drugs and Crime, 2013).

- Selgelid M.J. 'A tale of two studies: ethics, bioterrorism, and the censorship of science', (*Hastings Center Report*, 2007).
- Snegovaya M., 'Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare', (*ISW*, 2015).
- Statement of the Ministry of Foreign Affairs of the People's Republic of China on the Award of 12 July 2016 of the Arbitral Tribunal in the South China Sea Arbitration Established at the Request of the Republic of the Philippines, (*Chinese Journal of International Law*, 2016), 15(4).
- Study Group of the International Law Commission, 'Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law', (2016), Document A/CN.4/L.682 and Add.1, Available at: < https://legal.un.org/ilc/documentation/english/a_cn4_l682.pdf>, (accessed 26 July 2022).
- 'The Convention on Biological Diversity', in Secretariat of the Convention on Biological Diversity, (*Global Biodiversity Outlook*, 2001).
- The Council of the European Union, 'Council Conclusions on Cyber Diplomacy' 6122/15, Brussels, (2015).
- The European Parliament and the Council, 'Joint Communication: the EU's Cybersecurity Strategy for the Digital Decade', Brussels, (2020).
- The European Commission and HREU, 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', Brussels, (2013).
- 'The Global Risks Report 2019', (World Economic Forum 2019), Available at: <https://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf>, (accessed 24 May 2022).
- The Royal Society & The Royal Academy of Engineering, 'Nanoscience and Nanotechnologies: Opportunities and Uncertainties', (*The Royal Society*, 2004).
- The World Summit on the Information Society, 'Geneva Declaration of Principles and Plan of Action', Geneva, (2003), WSIS-03/GENEVA/DOC/4-E.
- Torossian B., Fagliano L., and Görder T., 'Hybrid Conflict - Strategic Monitor 2019-2020', (*The Hague Center for Strategic Studies*, 2021).
- Townsend-Drake A., 'Bioterrorism: Applying the Lens of COVID-19', (*Counter Terrorism Preparedness Network, 2021*).
- Trapp R., 'Compliance Management under the Chemical Weapons Convention', (*WMDCE*, 2019).
- Trenin D., 'Russia's National Security Strategy: A Manifesto for a New Era', (*Carnegie*, 2021).

- United Nations Security Council Counter-Terrorism Committee Executive Directorate, 'The Impact of the COVID-19 Pandemic on Terrorism, Counter-Terrorism and Countering Violent Extremism', (2020).
- UNEP, 'Implementation of the Convention and its Strategic Plan', (2016), Available at: <http://cbd.int/kb/record/decision/11020?RecordType=decision&Subject=STRAT>, (accessed 7 June 2022).
- United Nations, 'Forth Review Conference of the Parties to the Convention on the Prohibition, the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction: Report of the Committee of the Whole', Geneva, (1996), Available at: <https://docs-library.unoda.org/Biological_Weapons_Convention_-_Fourth_Review_Conference_(1996)/BWC_CONF.IV_06.pdf>, (accessed 14 June 2022).
- United Nations Office on Drugs and Crime, Malby S. and Davis P., 'Monitoring the Impact of Economic Crisis on Crime', (2012).
- US Senate Select Committee on Intelligence, 'Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations', (2018).
- Vice-President Ansip, 'The Chatham house annual cyber conference: evolving norms, improving harmonisation and building resilience. Speech by Vice-President Ansip', (2017).
- Viviane Reding, 'The EU's Data Protection Rules and Cyber Security Strategy: Two Sides of The Same Coin' (2013), Available at: <https://ec.europa.eu/commission/presscorner/detail/de/SPEECH_13_436>, (accessed 18 May 2022).
- WHO, 'IHR State Parties Self-Assessment Annual Reporting Tool', Available at: < https://apps.who.int/iris/bitstream/handle/10665/272432/WHO-WHE-CPI-2018.16-eng.pdf?sequence=>, (accessed 12 June 2022).
- WHO, 'Strengthening preparedness for health emergencies: implementation of the International Health Regulations (2005), (2021).
- WHO, 'Thematic Paper on the Status of Country Preparedness Capacities', (2019), Available at: <https://www.gpmb.org/annual-reports/overview/item/thematic-paper-on-the-status-of-country-preparedness-capacities>, (accessed 12 June 2022).
- WHO, 'Situation Report - 13' (2020), pp. 2, Available at: < https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf>, (accessed 21 May 2022).
- WTO, 'World Trade Report 2009: Flexibility in Trade Agreements', (2009).
- Xiong F., and others, 'Recognition and Evaluation of Data as Intangible Assets', (*Sage*, 2022).

- Ziolkowski K. 'Jus ad bellum in Cyberspace – Some Thoughts on the ‘‘Schmitt-Criteria’’ for Use of Force', (NATO CCD COE Publications, 2012).

Websites

- Barton G., 'Al Qaeda Near Biological, Chemical Arms Production', (*Washington Post*, 2003), Available at: < https://www.washingtonpost.com/archive/politics/2003/03/23/al-qaeda-near-biological-chemical-arms-production/8b88e5d0-5f00-4b3c-83a8-b396c0856d90/>, (accessed 29 August 2022).
- Byman D., 'Why Engage in Proxy War? A State’s Perspective', (*Brookings*, 2018), Available at: <https://www.brookings.edu/blog/order-from-chaos/2018/05/21/why-engage-in-roxy-war-a-states-perspective/>, (accessed 26 May 2022).
- 'CCDCOE To Host The Tallinn Manual 3.0 Process' (*Ccdcoe.org*, 2022), Available at: <https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/>, (accessed 9 May 2022).
- Council of Europe, 'Chart of Signatures and Ratifications of Treaty 185' (*Coe.int*, 2022), Available at: <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185>, (accessed 10 July 2022).
- Council of Europe, 'Tonga Joins the Budapest Convention on Cybercrime' (*Coe.int*, 2017), Available at: <https://www.coe.int/en/web/cybercrime/t-cy-news/-/asset_publisher/GxUcENEFhivB/content/the-kingdom-of-tonga-today-acceded-to-the-budapest-convention-on-cybercrime-to-become-the-55th-party-to-this-treaty-?inheritRedirect=false>, (accessed 13 July 2022).
- 'Ecommerce In Europe: €717 Billion In 2020' (*Ecommerce News*, 2020), Available at: <https://ecommercenews.eu/ecommerce-in-europe-e717-billion-in-2020/>, (accessed 23 May 2022).
- European Commission, 'Digital Economy and Society Index – DESI', (2021), pp. 15, available at: < https://digital-strategy.ec.europa.eu/en/policies/desi>, (accessed 15 May 2022).
- Frolovskiy D., 'What Putin Really Wants in Syria', (*Foreign Policy*, 2019), Available at: <https://foreignpolicy.com/2019/02/01/what-putin-really-wants-in-syria-russia-assad-strategy-kremlin/>, (accessed 26 May 2022).
- Gutierrez J., 'Philippines Officially Leaves the International Criminal Court', (*New York Times*, 2019), Available at: < https://www.nytimes.com/2019/03/17/world/asia/philippines-international-criminal-court.html>, (accessed 14 July 2022).

- Jovanovic B., 'A Not-So-Common Cold: Malware Statistics In 2022', (*Dataprot*, 2022), Available at: <https://dataprot.net/statistics/malware-statistics/>, (accessed 20 May 2022).
- Lawless, J. and Kirka, D., 'UK, US, Canada Accuse Russia of Hacking Virus Vaccine Trials', (*TechXplore*, 2020), Available at: <https://techxplore.com/news/2020-07-uk-canada-accuse-russia-hacking.html>, (accessed 13 July 2022).
- Ling J., 'The Lab Leak Theory Doesn't Hold Up', (*Foreign Policy*, 2021), Available at: <https://foreignpolicy.com/2021/06/15/lab-leak-theory-doesnt-hold-up-covid-china/>, (accessed 21 May 2022).
- Patterson D., 'Hackers Are Attacking The COVID-19 Vaccine Supply Chain', (*Cbsnews.com*, 2022), Available at: <https://www.cbsnews.com/news/covid-19-vaccine-hackers-supply-chain/ >,(accessed 25 May 2022).
- Pennisi E., 'Robotic Stingray Powered by Light Activated Muscle Cells', (*Science*, 2016), Available at: <https://www.science.org/content/article/robotic-stingray-powered-light-activated-muscle-cells>, (accessed 20 July 2022).
- Schmidt T., 'What the President's Interim National Security Strategic Guidance means for the U.S. Military', (*The Pacific Council magazine*, 2022), Available at: < https://www.pacificcouncil.online/commentary/opportunity-for-apolitical-military>, (accessed 3 June 2022).
- Steward J., 'The Ultimate List Of Internet Of Things Statistics For 2022' (*Findstack*, 2022), Available at: <https://findstack.com/internet-of-things statistics/#:~:text=Internet%20of%20Things%20(IoT)%20emerged,and%2075.44%20billion%20by%202025.>,(accessed 13 July 2022).
- The Economist, 'Improvised weapons. Hell's Kitchens', (2016), Available at: < https://www.economist.com/science-and-technology/2016/05/21/hells-kitchens >, (accessed 1 August 2022).
- The Hypocrisy of Russia's Push for a New Global Cybercrime Treaty' (*Lowyinstitute.org*, 2022), Available at: <https://www.lowyinstitute.org/the-interpreter/hypocrisy-russia-s-push-new-global-cybercrime-treaty>, (accessed 11 July 2022).
- The National People's Congress of the People's Republic of China, 'Data Security Law of the People's Republic of China', (2021), Available at: <http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml>, (accessed 24 June 2022).
- The State Council Information Office of the People's Republic of China, 'China's National Defense in the New Era' (Xinhua, 2019), Available at: <

https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html>, (accessed 15 June 2022).

- Ursula von der Leyen, 'Speech in The European Parliament Plenary Session', (*European Commission* 2019), Available at: < https://ec.europa.eu/info/sites/default/files/president-elect-speech-original_1.pdf>, (accessed 20 May 2022).
- Vipul Kharbanda, 'International Cooperation in Cybercrime: The Budapest Convention — The Centre for Internet and Society' (*Cis-india.org*, 2019), Available at: <https://cis-india.org/internet-governance/blog/vipul-kharbanda-april-29-2019-international-cooperation-in-cybercrime-the-budapest-convention>, (accessed 11 May 2022).
- WHO, 'Coronavirus (COVID-19) Dashboard' (*Covid19.who.int*, 2022), Available at: <https://covid19.who.int/>, (accessed 21 May).