The human beings have an ambivalent attitude towards technology, whereas nowadays technology represents not only a presence, but also a significant transformative force of human life, of human realities and, to a certain extent, of human nature itself. The collective volume entitled *Technology and International Relations. The New Frontier in Global Power* reunites a group of specialists in contemporary technological developments with impact in international relations and addresses the topic of technology as source of empowerment in the near future global power starting from the recognition of the current paramount importance of technology in the exercise and concentration of power (and wealth) in our world. The editors highlight a crucial aspect: "The centrality of technology as a tool for harnessing wealth and power in the twenty-first century is recognized outside the US and China. European Union member states – and the European Commission – have promoted awareness on the centrality of combining science and technology strategies in public policy discourses, planning and implementation, and research funds allocation." (p. ix) Even more, the argument shows that "European initiatives in civilian domain, such as those to promote so-called key-enabling technologies (micro- and nanoelectronics, nanotechnology, industrial biotechnology, advanced materials, photonics, and advanced manufacturing technologies) have been central to EU's industrial policy for a decade." (pp. ix-x) Technological developments take place at an alert pace, triggering organized political attention for this type of developments, which nature is transforming enough to change our historical perceptions, so that a decade becomes a "longer" and more significant duration than the historical perception of a decade during the 20th century.

The structure of the volume follows the areas of fast technological development. The first part is entitled "Technology and International Relations: Political, Economic and Ethical Aspects" and analyses technology as a catalyst of international power. J. Eriksson and L. Newlove-Eriksson provide an overview of the important aspects concerning the interrelation between technology and international relations in the first chapter – "Theorizing technology and international relations: prevailing perspectives and new horizons". The chapter emphasizes that the theories on technology in IR have developed starting from the main IR theories (realism, liberalism and constructivism), which have considered technology an exogenous factor in IR. "Techno-political studies have yet to make a significant mark in the IR, but they are making progress with regard to conceptualization of, for example, the fusion f new technologies with the social, the political and even the biological. There is also room for new theory and research both on such structural techno-political shifts and on the

politics of specific technologies, including AI, automated weapons and bioengineering." (p. 17)

The next chapter, "Mapping technological innovation", by Fr. N. Moro and M.Valigi, approaches the matters of intellectual property in technological innovation. Japan, US and China lead the technologically innovative fast track, followed by the EU countries. The study shows that the future challenge for states stays in the capitalization and administration of technological innovation in the light of benefices, costs and impact in IR. Technological change and innovation represents a problem-solving tool in relation to human resources and opportunities management and in relation to a mindset change. "This mindset change will require major reframing of human resources departments. The persons who will have to coordinate and manage such individuals would have to be 'different' themselves and (almost) equally innovative." (p. 41)

The topic of "Autonomy in weapons systems and its meaningful human control: a differentiated and prudential approach" by D. Amoroso and G. Tamburrini, concluding the first part of the volume, emphasize the necessity to have a meaningful human control (MHC) over the weapons systems, which makes compulsory the compliance with the international rules concerning the use of the lethal and sub-lethal weapons. The authors plea for a general principle of international law implying the necessity of human control over the weapon systems and propose an efficient methodology to evaluate the most relevant weapon systems and their MHC qualities. In what concerns the approach of the theme, we appreciate especially the focus on humanitarian aspects, responsibility and warrants of moral agency.

The second part of the volume is dedicated to "Robotics and Artificial Intelligence: Frontiers and Challenges". Chapter 4, titled "Context matters: the transformative nature of drones on the battlefield", by Sarah Kreps and Sarah Maxey, opens the discussion by the evaluation of the destabilizing role of the drones. Two main views on drones are identified: a more pessimistic one, emphasizing the lowering of the social barriers in society against the dispatching of long-distance lethal force weakening the public awareness (vigilance) concerning the potential human implications and deteriorating the protective (ethical) legal standards. The more optimistic view calls attention to the fact that drones are just another platform, less capacious than other technological platforms and posing less risk, since they

do not hold territories and they do not actually win wars. (pp. 69-70) Drones may gain positive roles in humanitarian and peacekeeping interventions, where their transformative roles are acclaimed. (p.77)

Technological progress in the field of robotics and AI indicates something close to an AI revolution. L. Martino and F. Merenda approach the theme "Artificial intelligence: a paradigm shift in international law and politics? Autonomous weapon systems as a case study" with the main concern for "the transformative role of the impact of AI on all aspects of our public and private life. In the IR and especially in military sector and activities worldwide the concern addresses the autonomous weapon systems (AWS), which differ from drones, precisely in this autonomy in initializing and finalizing a military action. Some of these may be knowledge-based systems, while others may be machine-learning systems, developed more recently, to perform tasks that are easy to perform for people, but difficult to describe. The lack of a internationally accepted and observed definition for AWS makes it difficult to impose an international body of laws and an international ethical code for these activities. We are at the stage of debate. Legal scholars advance arguments in favour or against the employment of AWS. Technological development might just significantly overcome the ruling and regulating developments.

Part three of the volume is titled "Space and cyberspace: intersection of two security domains". For more than half a century, the human race took international relations to the outer space. Luciano Anselmo, in the chapter dedicated to the issue of "The use of space and satellites: problems and challenges" starts the discussion from the observation that the outer space stage has been geopolitical in every way and it was mainly the stage for international competition and the activities in the outer space brought along more fallouts than cooperation. The outer space is both a global resource and an opportunity, both tensioned and disputed among national and international interests, between public and private interests. There is a growing technological production for space and a growing presence in space. "In 2018, for example, China carried out more orbital launches, 39, than any other country as compared with 31 by the United States, 20 by Russia and eight by Europe. It already spends more on its space projects than Russia and Japan, but still less than Europe combined, and much less than the United States." (p. 111) Although the first Space Age is overcome and the competition for Space among superpowers might not be the relevant characteristic in the future, right now, we witness the phenomenon of the assault of

the ambitious private commercial players, who conduct a technological revolution of the satellites and quasi touristic trips to the orbit. New problems emerge, nevertheless related to the safe and responsible use of space as a resource. “Moreover, while many of the military functions played by orbital systems could easily be replaced in the battlefield using other means and technologies (…) the maintenance of efficient global intelligence and surveillance capabilities through the conflict would be of paramount importance for reaching a truce (…).” (p. 117) Orbital debris poses serious problems, too. Certain land operations might as well generate complications. There are worries around the probability of space combat generated by unresolved IR tensions, although it is “considered neither advantageous nor probable within the strategic environment and the technology developments foreseen in the coming decades.” (p. 127)

“Cyber attacks and defenses: current capabilities and future trends”, by M. Colajanni and M. Marchetti, follows the evolutions and problems brought along by the digital revolution. The competitivity make it so that software industry delivered insufficiently tested products speculated by cyber criminals. The improvement is dependent on customers’ complaint and on cost efficiency on customers’ and companies’ respective parts. “Business models prevailing in modern digital society are based on ‘free’ services that are paid through data collection” (p. 133). Gray areas of data analytics emerge and they are speculated by cyber criminals and shady opportunists. Cyber defences are difficult, due to the lack of specialists, and ethical and legal vulnerabilities.

The need for complex security seems to be the hallmark of our times. Andrea Locatelli argues in the next chapter, “Critical infrastructure protection”, for an optimal balance between functional security and territorial security. Simply put, national security depends on society’s ability to deliver (and access) certain significant, important and vital goods and services. Banking and finances, communications, emergency services, energy, water supply systems, food and agriculture, healthcare, commercial facilities, chemical sector, manufacturing facilities, dams, defence industrial base, information technologies, government facilities, nuclear material, transportation, all these, represent national critical infrastructures, which should be defended and well-managed as a priority matter of national security. Natural hazards, human error, technological failure, cyberattacks or deficient public-private partnerships are main illustrations for the many threats to critical infrastructure. The study approaches the case studies of the United States and the

European Union, following the main models and stages in critical infrastructure security matters. The conclusion shows that "technological remedies are a necessary but not sufficient condition to guarantee protection, human skills being equally if not more important" and system vulnerabilities make offence easier than defence (p. 168).

"A perfect storm: privatization, public-private partnership and the security of critical infrastructure" by Giampiero Giacomello continues the analysis of the previous chapter at a different level, giving a special status to critical information infrastructures in relation to all critical infrastructures, since they may become main vulnerabilities and weapons in computer network attacks against other critical infrastructures. "Modern societies would demand that a 'balance' of anticipation and resilience policies be applied to solving the problems exposed and protecting CII (the critical information infrastructure)." (p. 186) Effective security requires effective anticipation of risks, the protective separation of every critical infrastructure, the recognition of priority for public security interests in healthy private-public partnerships. "Ultimately, that cybersecurity should become everyone's concern is somehow inevitable". (p. 187) Investing in CIIs' protection becomes more and more necessary, as the current COVID-19 experience has shown. The stakes we have in technological security, safety and protection are nowadays ever clearer.