BOOK REVIEW: K. MICHALSKI, M. JURGILEWICZ, KONFLIKTY TECHNOLOGICZNE. NOWA ARCHITEKTURA ZAGROŻEŃ W EPOCE WIELKICH WYZWAŃ

ŁUKASZ SZYMANKIEWICZ, PHD
ORCID: 0000-0002-9859-9896
WSB University in Dąbrowa Górnicza, Poland

Will the escalating social controversies and conflicts over technological innovations soon lead to a paradigm shift in technical safety management? (Book review by K. Michalski, M. Jurgilewicz, *Konflikty technologiczne. Nowa architektura zagrożeń w epoce wielkich wyzwań*, Difin, Warsaw 2021, pp. 1-251).

The development of information and communication technologies and the growing importance of the security of the infosphere and cyberspace, the global technological race and the need to build an advantage thanks to the rush implementation of innovations, before science fully recognizes their consequences, internationalization and globalization – gradual elimination of migration barriers limiting the flow of capital, information, goods and people – opening new opportunities for expansion and fostering the emergence of new dimensions of complex interdependencies, progressive environmental degradation, disruption of the ecological balance, climate change and an increase in threats to public health, including epidemic threats, and the progressive erosion of the traditional system of representative democracy, and an increase in the activity and importance of supranational organizations and non-governmental initiatives – these are undoubtedly the main megatrends shaping the contemporary security environment, both internationally and internally in countries (see Aleksandrowicz 2020). There are complex interactions and synergies (mutual reinforcements) on many levels between all these processes, creating one-dimensional security analyzes, assessments and strategies – limited to single domains and based on threat elementarization – less and less cognitively adequate and less useful in practice. In the face of the current civilization changes, there is a growing awareness in many circles of a new type of structural threats resulting from the rapidly growing complexity of security ecosystems, mainly due to the technological boom. More and more often we hear postulates related to the need to change the current paradigm in security policy, the pillars of which are the Aristotelian substantialist ontology based on the concept of things, a Cartesian model of scientific cognition that considers reducing complex issues to “clear and distinct ideas” as the right way to understand complexity, inspired by Newtonian deterministic-linear concept of causality, based on it individualistic-linear understanding of responsibility widespread in voluntarist legal systems and ethical doctrines of Latin civilization and supplemented by Cartesian methodical skepticism, imposing the presumption of innocence in the absence of compelling scientific evidence for the existence of mutually unambiguous cause-effect relationships, as well as the boundless belief in the computability of the world and the recognition of computability as the only objectivizing strategy, which results in excessive quantitative research. The fateful effect of these philosophical assumptions is the widespread belief in the safety promises made by commercialized laboratory science, and the widespread depreciation of alternative models of cognition, contemptuously referred to as pseudo- or para-science – and when such nomenclature does not help, labelling with conspiracy theory is an effective means of silencing the unrighteous, which is only a short step away from accusations of terrorism. The falsity of these assumptions, which are the "founding myth" of the Western European security culture, are interestingly exposed by the authors of the book *Konflikty technologiczne. Nowa architektura zagrożeń w epoce wielkich wyzwań*, published in March 2021 by the Warsaw publishing house Difin as part of a series dedicated to security sciences.

As technology and technological innovation are widely regarded as a blessing in the modern world, technological threats and risks are rarely the subject of research in mainstream security science (securitology). If technological issues appear on the security conferences agendas, they are usually considered in terms of a possible imbalance of power, and the source of security problems is more often seen in their scarcity than in technologies. The authors of the book warn of the dire consequences of such a one-sided, overly optimistic view of technology only as a boon – a major factor in growth and strategic advantage. Krzysztof Michalski – scientist and methodologist from Rzeszow University of Technology, specializing in technology assessment and interdisciplinary security analyzes, and Marcin Jurgilewicz – lawyer and political scientist from Rzeszow University of Technology, specializing in research in the scope of public safety and order, especially assembly safety, the use of direct coercion measures, conflict resolution and anti-crisis measures – indicate new dimensions of threats to internal security resulting from inappropriate technological policy. The authors of the book see the source of primary threats not only in the multifaceted ambivalence of technology, but also in the rapidly growing structural complexity of technical systems (mainly due to hybridization related to the transformation of these systems into cyber-physical systems, as well as their growing network). Increasing complexity gives technical systems the ability to self-organize and operate autonomously without our knowledge and against human will. The authors of the book note that in the face of the growing dependence of the modern network society on the reliability of technology in increasingly simpler life activities and the increasingly collective, "totalitarian" nature of technologies, from which there is no escape from harmful or dangerous effects, there is growing distrust in many social circles of (some) technologies and fear of the vicinity of various types of industrial installations (NIMBY). The mistrust and fears of the population are fueled not only by the increasingly less credible security promises made by increasingly commercializing laboratory sciences and increasingly questioned by technological disasters, failures and space-time unlimited chains of damage, but also malicious disinformation activities in cyberspace carried out by hostile organizations with the intention of causing widespread disorientation, internal splits, conflicts and political crises capable of threatening the security and stability of states.

Michalski and Jurgilewicz reveal to the reader surprising constellations of interests in maintaining the security of technical systems at the lowest possible level. This dangerous alliance is created primarily by technological enterprises (1) forced by increasing competition to implement innovations before science fully recognizes their impact on people and the environment, commercialized science (2) legitimizing risky innovations by systematically producing doubts as to their social harmfulness, the so-called risk industry (3) – a high-margin, multi-industry branch of production and services (insurance, protection measures, security systems, claims handling and reconstruction, etc.) benefiting from misfortunes that arouse additional security needs in society, as well as state authorities (4) – in principle, favorable to dangerous business ventures, because they tax the related financial flows, and the legal systems existing in most countries (5), based on linearly understood, individual, retrospectively oriented responsibility, "after damage" response and the principle of presumption of innocence in the absence of compelling evidence of individual fault.

All these conditions work – according to the authors – to the benefit of those who risk and put into question the effectiveness of administrative supervision over the safety of projects, devices, products and processes. The growing social awareness of these conditions, which guarantee the high susceptibility of modern industrialized societies to catastrophes, causes a change in people's attitudes towards technological achievements in many countries. The authors of the book express concerns that social controversies and conflicts over technological innovations, resulting from improper conduct of technological policy "behind closed doors", without the participation of stakeholders, will soon become a factor in any civil society that seriously disrupts the processes of economic development and threatens the internal security of countries and their position in the international arena. Therefore, they are looking for solutions that will be able to effectively eliminate such conflicts "at the source" or limit their destructive impact on the processes of technological development, the continuity of which determines the national welfare, stability and security of states, and the competitiveness of economies. Michalski and Jurgilewicz indicate three necessary conditions for rational and socially responsible handling of technological conflicts:

1) Preventing technological conflicts in the conditions of the increasingly totalitarian nature of modern technological innovations requires the empowerment of citizens. Decisions on the choice of technology and the implementation of socially controversial technological projects taken at various levels of public administration and in enterprises should be preceded by a reliable technology assessment taking into account the full spectrum of social consequences and open to fair participation of all stakeholders possible. A sense of being heard and genuinely co-decid-

ing makes socially agreed decisions binding for everyone from within, not perceived as imposed from outside.

2) In order to reduce organized irresponsibility in corporations – both in technological enterprises, scientific and research institutions certifying the safety of projects, devices, products and processes, and in administrative supervision authorities – and to restore public confidence in the decision to implement or abandon a specific technology, a statutory obligation should be introduced to install credible internal anti-corruption systems (including whistleblowing) in all public interest organizations, the deterrent power of which is confirmed by the pioneering experience of several countries.
3) It is necessary to seek amicable resolution or de-escalation of technological conflicts, which for various reasons could not be prevented. A method with an optimal balance of advantages and disadvantages in relation to technological conflicts is mediation and its "crossovers" with other ADR (alternative dispute resolution) formulas. The last chapter of the book, the authors devoted to a detailed discussion of the conditions for the success of mediation in typical conflict situations that accompany location decisions, implementation of infrastructure projects and decisions on allowing technological solutions that cause social controversy, as well as an analysis of the legal limitations of the use of mediation in solving this type of complex multi-agent conflicts. structure in the Polish reality.

The analysis of the genesis of a new type of threats to the internal security of states and the recipes for building lasting peace around technological ventures of strategic importance for sovereignty, economic competitiveness and civilization development proposed by the authors of the book may serve as signposts for decision-makers representing various levels of public administration and various industries. The added value of the publication is mostly a foreign-language source base, introducing threads and content to Polish scientific discussion so far known only to a very narrow circle of specialists. A lively, popular-scientific narrative style, interwoven with intriguing questions and provocative theses prompting a deeper reflection on contemporary technical practice, makes a scholarly book about the intricacies and paradoxes of security policy an engaging reading accessible to laymen. As the book signals momentous problems that concern everyone and contains more questions than answers, it has the potential to initiate a society-wide discussion that will lead to a much-needed reductionist paradigm shift in the approach to the security of technical systems.