Politeja
No. 4(79), 2022, pp. 5-16
https://doi.org/10.12797/Politeja.19.2022.79.01

Artur GRUSZCZAK
Jagiellonian University in Kraków
artur.gruszczak@uj.edu.pl

Mateusz KOLASZYŃSKI
Jagiellonian University in Kraków
mateusz.kolaszynski@uj.edu.pl

UNDERSTANDING CONTEMPORARY SECURITY

A PROLEGOMENON TO THE INTERPLAY BETWEEN TECHNOLOGY, INNOVATION AND POLICY RESPONSES

ABSTRACT Contemporary security is shaped by a variety of factors which determine the changing dynamics of connections and interdependencies within and between social groups and political actors. The growing importance of technology and innovation for states and societies has been a critical factor in the infrastructural, organizational and decision-making dimensions. This article aims to integrate some aspects of contemporary security into current dynamics of technology and innovation as vehicles of rapid and substantial changes in security policies and actions. Designed as an essay based on qualitative method in social sciences, this paper raises theoretical and empirical questions concerning modernization and innovation as determinants of contemporary security structures and policies. The empirical dimension of technology, innovation and politics are presented in the microscale (local security), in the mesoscale (state security, national security, sectoral security) and in the macroscale (international security in regional and global dimensions), as well as from the cross-sectional (transversal) perspective.

Keywords: security, technology, innovation, modernization, policy response

I

Contemporary security is a form of social relations exceptionally susceptible to both sudden, unexpected events and long-term processes of transformations and changes taking place in many dimensions of social interactions. Research in, conceptualization, and understanding of security must take into account the changing dynamics of varied forms of societal organization, connections and interdependencies within and between social groups, as well as the growing importance of technology and innovation in the infrastructural, organizational and decision-making dimensions.[1] Taking into consideration the variety of factors shaping contemporary security, special attention should be paid to those which determine, stimulate and often enforce deep, structural changes in societies, in their cultures and customs, as well as forms of power and institutions of governance.

This article makes an endeavor to integrate aspects of contemporary security into current dynamics of technology and innovation as vehicles of rapid and substantial changes in security policies and actions. We refer to this as a prolegomenon because we believe that theoretical and empirical discourses on security have failed to sufficiently problematize the interplay between technology-driven innovation and policy responses to the complex outcomes of research, development and innovation fostered by security imperatives. We pretend to address this deficiency in an introductory manner, suitable for the convention of an article opening a series of papers engaging with varied aspects of the topical trinitarian relation. Therefore, we hope this prolegomenon also helps to understand the complexities and intricacies of security-related questions raised in the present thematic issue on technology, innovation and policy responses.

This paper has the form of an essay based on qualitative method in social sciences, and security studies in particular, in which theoretical and empirical issues of modernization and innovation as determinants of contemporary security are put together. Technologies will be considered both as solutions to the observed problems through the use of specific methods, techniques and tools, as well as innovation bases aiming to cause qualitatively significant changes in the nature and structure of reality. They will also be seen as catalysts for political action, especially when their effects are transferred to power relations and governance structures. The empirical dimension of technology, innovation and politics may be presented in the microscale (local security), in the mesoscale (state security, national security, sectoral security) and in the macroscale (international security in regional and global dimensions), as well as from the cross-sectional (transversal) perspective. Inter- and transdisciplinary analyses may bring additional methodological, cognitive and explanatory values of the study of contemporary security.

[1] See N. Elias, "Technization and Civilization", *Theory, Culture & Society*, vol. 12, no. 3 (1995); R. Bellanova, K. Lindskov Jacobsen, L. Monsees, "Taking the Trouble: Science, Technology and Security Studies", *Critical Studies on Security*, vol. 8, no. 2 (2020).

II

Technologies should be considered as the variable which, to a large extent, determines the development of humanity in the late Anthropocene[2] and draws the boundary conditions and the logic of the evolution of the human-created and human-sustained ecosystem.[3] It is technology that sets the directions for the development of technical infrastructure, which structures network connections in the social, economic, political and ideational dimensions. It underpins communication and exchange, and above all, it leads to the virtualisation of social relations in cyberspace. The latter effect was explicitly addressed by scholars and experts in the early stage of the expansion of cyberspace.[4] However, Dominika Dziwisz advances in the present issue of *Politeja* a bold thesis that doomsday scenarios of a 'cyber Pearl Harbor'[5] are unlikely to come true due to the anchorage of cyber operations in the gray zone activities which tend to be kept under the threshold of a formally declared conventional war.[6] This does not mean that cyberspace can be underestimated as a dimension of contemporary security. Rather, this argument points to a discrepancy between the present concepts of warfare along with their application in local conflicts and international competition, and the breathtaking pace of advancements in military and defense technologies.[7] Progress in emerging technologies for warfighting has been ceaseless and inexorable, expressed in such fields as (lethal) autonomous weapon systems,[8] weaponization of biotechnologies, directed-energy weapons and hypersonic weapons. The

2 B. Szerszynski, "The End of the End of Nature: The Anthropocene and the Fate of the Human", *The Oxford Literary Review*, vol. 34, no. 2 (2012).

3 M. Fagan, "Security in the Anthropocene: Environment, Ecology, Escape", *European Journal of International Relations*, vol. 23, no. 2 (2017); E. Cudworth, S. Hobden, "Beyond Environmental Security: Complex Systems, Multiple Inequalities and Environmental Risks", *Environmental Politics*, vol. 20, no. 1 (2011).

4 M. Heim, *The Metaphysics of Virtual Reality*, New York 1993; S.G. Jones (ed.), *CyberSociety: Computer-Mediated Communication and Community*, London 1995; D. Holmes, "Introduction: Virtual Politics – Identity and Community in Cyberspace", [in:] D. Holmes (ed.), *Virtual Politics: Identity and Community in Cyberspace*, London 1997; M. Margolis, D. Resnick, *Politics as Usual: The Cyberspace 'Revolution'*, London–Thousand Oaks–New Delhi 2000.

5 See S. Lawson, M.K. Middleton, "Cyber Pearl Harbor: Analogy, Fear, and the Framing of Cyber Security Threats in the United States, 1991-2016", *First Monday*, vol. 24, no. 3-4 (2019); J. Straub, "Defining, Evaluating, Preparing for and Responding to a Cyber Pearl Harbor", *Technology in Society*, vol. 65 (2021), 101599; H.Ch. Turner, "Cyber War Forthcoming: »It Is Not a Matter of If, It Is a Matter of When«", E-International Relations, 8 July 2020, at https://www.e-ir.info/2020/07/08/cyber-war-forthcoming-it-is-not-a-matter-of-if-it-is-a-matter-of-when/, 28 July 2022.

6 Compare T. Rid, "Cyber War Will Not Take Place", *Journal of Strategic Studies*, vol. 35, no. 1 (2012); J. Stone, "Cyber War *Will Take Place!", Journal of Strategic Studies*, vol. 36, no. 1 (2013).

7 See Ł. Kamieński, *Mimowolne cyborgi. Mózg i wojna przyszłości*, Wołowiec 2022; K.M. Sayler, "Emerging Military Technologies: Background and Issues for Congress", Congressional Research Service, 6 April 2022, at https://sgp.fas.org/crs/natsec/R46458.pdf, 27 July 2022.

8 See P. Scharre, *Army of None: Autonomous Weapons and the Future of War*, New York 2018; A. Rossiter (ed.), *Robotics, Autonomous Systems and Contemporary International Security*, London–New York 2021.

latter is thoroughly depicted in this thematic issue by Marek Czajkowski, who argues that hypervelocity technologies, despite limitations and shortcomings of their implementation, are supposed to alter the existing strategic security balance, and as such have become an arena of competition between the major global powers.

Technologies have opened up the field for the expansion of devices and systems based on artificial intelligence-driven algorithms with increasing machine learning capabilities, for the virtualization of a significant part of the economy and finance sectors, distance learning and remote self-education, and for cultural diffusion of incredible speed and scale of impact.[9] Quantum technologies employed in computing and communication introduce new capabilities, improve effectiveness of the *sensor*-to-*effector* cycle and increase precision of weapon systems, thus foreshadowing 'quantum warfare'.[10] In a similar vein, the progress in robotics, remote sensing and engine and powertrain systems has brought about a massive use of unmanned vehicles, especially in high-risk areas and zones of armed conflicts.[11] The use of unmanned aerial vehicles (UAVs, commonly termed as drones), initially for surveillance, observation and targeting, but next for attacking and liquidating adversaries, has shaped the modern warfare as decisively as cyber technologies. The fiercely debated 'drone wars' and 'targeted killings' have on the one hand raised ethical and humanitarian issues, yet on the other hand heralded a new element in contemporary security landscape, i.e., remote warfare marking a significant shift from the boots-on-the-ground axiom to granular time-sensitive above-the-ground kill boxes.[12] Hubert Królikowski in his article discusses a variety of technological, systemic and combat-driven features of the UAVs displayed during the armed conflicts in Syria, Libya and Nagorno-Karabakh, as well as – importantly – in Ukraine prior to the full-scale Russian military invasion in 2022. He convincingly argues that armed drones should not be identified with a 'lone gunslinger'. They are effective as parts of the command and control system integrated with surveillance, reconnaissance and target acquisition heavy reliant on real-time data acquisition and processing.

The development of information technologies has not been a key factor in the evolution of contemporary warfare in a multi-domain battlespace. It also has offered considerable advantages in terms of innovative research models in the field of security research through the use of cutting-edge methods from applied mathematics and computer science, such as network analysis, natural language processing, and machine

[9] N. Panteli, M. Chiasson (eds), *Exploring Virtuality within and beyond Organizations: Social, Global and Local Dimensions*, Basingstoke 2008.

[10] M. Krelina, "Quantum Technology for Military Applications", *EPJ Quantum Technology*, vol. 8 (2021), art. 24.

[11] See the classical books by P.W. Singer (*Wired for War: The Robotics Revolution and Conflict in the 21st Century*, New York 2009), A. Bousquet (*The Eye of War: Military Perception from the Telescope to the Drone*, Minneapolis 2018) and D. Sloggett (*Drone Warfare: The Development of Unmanned Aerial Conflict*, Barnsley 2014).

[12] See G. Chamayou, *A Theory of the Drone*, transl. by J. Lloyd, New York 2015. Compare C. Enemark, *Armed Drones and the Ethics of War: Military Virtue in a Post-Heroic Age*, London 2014; K.R. Himes, *Drones and the Ethics of Targeted Killing*, Lanham, MD 2016; P.L. Bergen, D. Rothenberg (eds), *Drone Wars: Transforming Conflict, Law, and Policy*, Cambridge 2015.

learning.[13] The matter of application of mathematical and algorithmic methods is discussed by Mateusz Kolaszyński and Dariusz Stolicki, who analyze the legislative process of surveillance law in Poland using quantitative methods for two purposes: to discover connections and relationships across large datasets, such as all bills proposed in the Polish parliament since 1990 (over 8000 items), parliamentary debates since 1990 (over 160 million words), and committee hearings since 1990 (over 60 million words of transcripts and over 12 million words of summary reports), etc., and to identify latent patterns in the data that would otherwise evade detection. Computerization has also opened up the field for the development of qualitative methods. Amelia Hutyra and Błażej Sajduk present the results of analysis of the contents of selected strategic documents concerning national security adopted by the United States and Poland between 2001 and 2021 using a software program designed for computer-assisted qualitative (MAXQDA Analytics Pro).

III

The above remarks should not be considered as an uncritical praise of technology as a critical factor for the fate of contemporary states and societies. Rather, they should be read as the pointing to that dimension of reality which causes far-reaching changes, entailing positive effects and carrying numerous risks, and even immediate threats. Technology and innovation bring about the growing asymmetry of the modern world, the deepening of structural disproportions and divisions between regions and countries, as well as within societies. Marginalization or exclusion increase the probability of dissent and rebellion and may be the source of disputes and conflicts.[14] The cultural premises of modernization and innovation contradict traditional systems of values, norms and patterns of behavior. Counter-modernization social movements can quite easily and quickly accumulate a significant potential for dissatisfaction and resistance, which may undermine public order and weaken the security of the state, or even destabilize the international arena.[15]

We used to acclaim that we are part of risk society in a self-endangering civilization.[16] Fears and anxieties which haunted nations, societies, ethnic and religious groups

[13] F. Mérand, S.C. Hofmann, B. Irondelle, "Governance and State Power: A Network Analysis of European Security", *Journal of Common Market Studies*, vol. 49, no. 1 (2011); A. Vestby, J. Vestby, "Machine Learning and the Police: Asking the Right Questions", *Policing. A Journal of Policy and Practice*, vol. 15, no. 1 (2019); I.H. Sarker, M.H. Furhad, R. Nowrozy, "AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions", *SN Computer Science*, vol. 2 (2021), art. 173.

[14] See B. Fuerst-Bjeliš, W. Leimgruber (eds), *Globalization, Marginalization and Conflict: Political, Economic and Social Processes*, Cham 2020; E. Vincze, A. Bartha, T. Virág, "Theoretical Potential of Addressing Production of Marginality at the Crossroads of Spatial Exclusion and Development", *Intersections: East European Journal of Society and Politics*, vol. 1, no. 4 (2015).

[15] See M.J. Mazarr, *Unmodern Men in the Modern World: Radical Islam, Terrorism, and the War on Modernity*, Cambridge 2007.

[16] U. Beck, *Risk Society. Towards a New Modernity*, London 1992, p. 10.

and various social communities have multiplied along with the accelerated pace of modernization and globalization. The catalogue of the main risks and threats was enriched every year from the beginning of the 21st century. Reported by numerous analytical institutions and think tanks, it occasionally hit the headlines and drew attention of the global audience. Terrorism, climate change, cyber threats, rising powers, pandemics, hybrid wars and transnational criminal networks were listed as factors posing complex challenges to global security in the strategic dimension.[17] It was widely understood that these risks and threats have anthropogenic sources, they result from human-made activities causing harm to the natural planetary equilibrium and to global commons pooled in the process of modernization and development. In that context, one can subscribe to Ulrich Beck's argument that: *Modern society has become a risk society in the sense that it is increasingly occupied with debating, preventing and managing risks that it itself has produced*.[18]

Modernization and innovation have become synonymous with continuous development, progress, as well as the increasing well-being of societies and the potential of countries which actively participate in the technological race and skillfully implement new systemic solutions.[19] The cultural and civilizational contradictions of modernization and innovation trigger specific political actions. The institutions of state power are responsible for keeping order, enforcing the law and guaranteeing the inviolability of the foundations of sovereign statehood. At the same time, state institutions are responsible for effective governance and a proper management of the public sphere. Decision-making processes link effective management with its social (civic) legitimacy. Consequently, risk management, threat prevention and the fight against advanced threats are based on balancing social needs and expectations with the possibilities of action on the part of the state. This aspect is considered in two articles in the current issue of *Politeja* in the microscale (local security). Paulina Polko analyzes the National Map of Security Threats (Krajowa Mapa Zagrożeń Bezpieczeństwa, KMZB) implemented in Poland as a GIS-based tool to involve citizens in creating local security and to have a source of knowledge about the perception of personal safety by KMZB users. In turn, Agnieszka Polończyk offers a spatial analysis of selected types of crime committed in the city of Krakow in the years 2017-2021. Her analysis is based on the local inspection of places defined as 'hot spots' in terms of their functional, spatial, and situational conditions conducive to or hindering the commission of crimes. Technologies of power and governance are gaining importance as factors which regulate the behavior of social actors and steer the infrastructure. Anticipatory governance, discussed by Maciej Stępka in the context of the EU's capacity to manage migration crises,[20] offers a more holistic approach to security, seeking to merge policy response with crisis management, recovery,

[17] See A.J. Masys (ed.), *Security by Design: Innovative Perspectives on Complex Problems*, Cham 2018.

[18] U. Beck, "Living in the World Risk Society", *Economy and Society*, vol. 35, no. 3 (2006), p. 332.

[19] See J. Cantwell, T. Hayashi (eds), *Paradigm Shift in Technologies and Innovation Systems*, Cham 2019.

[20] M. Stępka, *Identifying Security Logics in the EU Policy Discourse: The 'Migration Crisis' and the EU*, Cham 2022.

preparedness and prevention. In his paper Stępka suggestively argues that anticipatory governance interlocks with resilience in search of an effective mode of responding to security issues and mitigating unforseen consequences of security deficits.

IV

Policy responses in the modern conception of security used to combine and integrate – if possible or necessary – the reactive approach with the proactive, anticipatory stance. Anticipation is occupying a prominent place in the security governance system, including crisis management, for it facilitates situational assessment and contributes to optimization of decision-making processes.[21] It also involves the meaning and application of the concept of risk. Shunning from the discussion of this concept because of a plethora of its contexts, meanings and understandings, we indicate that risk increasingly affects policy responses to security challenges and may have a considerable impact on innovation as an expression of the state's adaptation to the changing security environment. We concur with Beck's argument, that risks exist in a permanent state of virtuality, and become 'topical' only to the extent that they are anticipated.[22]

Anticipation and risk management need accurate data and reliable information in order to foresee the dynamic of developments and forewarn decision makers of the coming (or looming) crises. This tackles the problem of collection, collation and integration of data and information which tend to be scattered over various sources, bases and repositories. This is one of the indicators of innovation and agility in data processing and intelligence in particular.[23] Data fusion is one of possible solutions to that problem and it is examined by Artur Gruszczak using the example of the EU's intelligence capabilities in the common security and defense policy. It is taken for granted that intelligence is key to preparedness, early warning, resilience building, crisis management and defense in the face of armed aggression. The recent dramatic developments in Ukraine have proven that intelligence assets, domestic and allied, were critical for the preparation of relevant Ukrainian forces and services for the Russian full-scale military invasion of 24 February 2022 and for thwarting of the plan to quickly capture the capital city of Kiev. Those assets were also utilized to take advantage of mistakes and failures committed by the Russian Federal Security Service (FSB).[24]

---

21 See B. Malakooti, "Decision Making Process: Typology, Intelligence, and Optimization", *Journal of Intelligent Manufacturing*, vol. 23, no. 3 (2012).

22 U. Beck, "Living in the World...", p. 332.

23 See J.J. McGonagle, C.M. Vella, *Proactive Intelligence: The Successful Executive's Guide to Intelligence*, London 2012.

24 P. Sonne et al., "Battle for Kyiv: Ukrainian Valor, Russian Blunders Combined to Save the Capital", *The Washington Post*, 24 August 2022, at https://www.washingtonpost.com/national-security/interactive/2022/kyiv-battle-ukraine-survival/?itid=na_top_nav, 26 August 2022; G. Miller, C. Belton, "Russia's Spies Misread Ukraine and Misled Kremlin as War Loomed", *The Washington Post*, 19 August 2022, at https://archive.ph/97QJv, 26 August 2022.

Lessons learned from the war in Ukraine, regardless of their tentative use for the analysis of that conflict, along with its repercussions for European security and the world order, have demonstrated the prominent role of the comprehensive approach to contemporary defense, security and crisis management. It has been preferred in security strategies and military doctrines of the leading Western powers, and it was adopted by the two principal security organizations of the West: NATO and the European Union.[25] It put the emphasis on the planning by education, training, and exercises; on coherence of actions, including civilian-military interactions in the areas of conflict and instability; organizational collaboration and political dialogue with external partners and an adequate strategic communication, wisely addressing the most sensitive aspects of military operations, especially with regard to the use of force. Eugeniusz Cieślak adopts a regional perspective on the development of Estonian, Latvian, and Lithuanian defense concepts. He focuses on the implementation of comprehensive defense concepts in the post-2014 period, when the efforts of the Baltic States intensified in response to Russian aggression against Ukraine and the illegal annexation of Crimea. He argues that all Baltic States have taken steps to implement a model of a comprehensive (total) national defense, significantly extending the scope of involvement in national defense of the non-military sector, as well as society. His contribution has an interesting corollary for the general discussion about total defense concepts and their utility in the confrontation with hybrid threats and gray-zone activities.[26] Despite unquestionable advantages and opportunities of the comprehensive/total defense concepts and models, some alternative organizational and institutional solutions may be applied as well, depending of the availability of military assets and structural properties of a defense system. This applies to countries like Poland who has grappled with the restructuring of the defense sector in the past years. A decentralized military defense in Poland is detailed by Agata Mazurkiewicz who assesses the potential for innovation of a mixed type of force in non-military crisis response by reviewing the key characteristics and actions carried out by the Territorial Defense Forces.

V

Faith in liberal order, international institutions, security alliances, safeguards and checks was drastically undermined by the blunt military aggression of the Russian Federation against Ukraine in February 2022. This blatant act of violation of fundamental norms

[25] D. Driver, "The European Union and the Comprehensive Civil-Military Approach in Euro-Atlantic Security: Matching Reality to Rhetoric", *Strategic Studies Quarterly*, vol. 4, no. 3 (2010); C. Major, Ch. Mölling, "More Than Wishful Thinking? The EU, UN, NATO and the Comprehensive Approach to Military Crisis Management", *Studia Diplomatica*, vol. 62, no. 3 (2009), pp. 21-28.

[26] J.K. Wither, "Back to the Future? Nordic Total Defence Concepts", *Defence Studies*, vol. 20, no. 1 (2020); I. Bērziņa, "From 'Total' to 'Comprehensive' National Defence: The Development of the Concept in Europe", *Journal on Baltic Security*, vol. 6, no. 2 (2020); G.J. Stein, "Total Defense: A Comparative Overview of the Security. Policies of Switzerland and Austria", *Defense Analysis*, vol. 6, no. 1 (1990).

of international law was followed by a series of hostilities not only against Ukraine, but also against the international coalition of Western allies strongly opposing Moscow's destructive strategy and condemning Russia for atrocities and war crimes committed in many places of the occupied lands of Ukraine. The military invasion of Ukraine should be perceived in the category of a catastrophe. This refers not just to the consequences of Russia's decisions and actions, direct disastrous effects in Ukraine, as well as mid- and long-term damage done to world security, international relations, global economy and – last but not least – public order. This is about – following Claudia Aradau and Rens van Munster[27] – a particular way of governing future events which we cannot predict but which may strike suddenly, without warning, and cause irreversible damage. The question of policy responses to Moscow's moves and its wide-range consequences seems to be a key factor in handling the conflict-resolution conundrum and predicting the shape of post-war things in Ukraine, Russia and the world. Recalling again Beck, we take seriously into consideration his distinction between risk and catastrophe. He wrote: *Risk does not mean catastrophe. Risk means the anticipation of catastrophe*.[28]

Contemporary security has been a process unfolding in a more and more complex environment where a plethora of actors resort to the increasingly sophisticated means, methods and instruments in order to pursue their intents and objectives. The technological factor is a critical variable in the advancement of information and intelligence systems, as well as top-level command and control networks driven by artificial intelligence and autonomous steering solutions. Therefore, innovation is a mandatory component of security building, crisis management and public order, seeking to fill structural and functional gaps in the existing networked architecture linking the international system, sovereign nation-states, social groups and individuals. However, such pressure on innovation and modernization may provoke a backlash from those actors who are the ultimate losers and who modify their policy responses in order to mitigate the negative consequences of technological race. This is suggestively described in the article by Dariusz Kozerawski, who makes a balance of the Western military intervention in Afghanistan through the lens of the Polish contingent. It also proves that asymmetry, typical for the irregular wars in the 21st century, is a product of indelible contradiction between technology-driven innovation and constructive policy responses in underdeveloped countries and their divided societies.

The mosaic of articles contained in this special issue show that a contemporary discourse on security zooms in on topics which determine the dynamics of security processes and should be considered as drivers of tremendous forces that shape the security environment now and in the future. The understanding of contemporary security consists in the ability to distinguish active and vibrant structures of innovation-driven actors, systems and solutions from a static background created by petrified patterns and forms of culture and organization. Ultimately, any policy response will suffer from indeterminacy and risk of failure, especially if violence and force are applied.

---

27 C. Aradau, R. van Munster, *Politics of Catastrophe: Genealogies of the Unknown*, London 2011.

28 U. Beck, "Living in the World...", p. 332.

BIBLIOGRAPHY

Aradau C., Munster R. van, *Politics of Catastrophe: Genealogies of the Unknown*, London 2011, https://doi.org/10.4324/9780203815793.

Beck U., "Living in the World Risk Society", *Economy and Society*, vol. 35, no. 3 (2006), pp. 329-345, https://doi.org/10.1080/03085140600844902.

Beck U., *Risk Society. Towards a New Modernity*, London 1992.

Bellanova R., Lindskov Jacobsen K., Monsees L., "Taking the Trouble: Science, Technology and Security Studies", *Critical Studies on Security*, vol. 8, no. 2 (2020), pp. 87-100, https://doi.org/10.1080/21624887.2020.1839852.

Bergen P.L., Rothenberg D. (eds), *Drone Wars: Transforming Conflict, Law, and Policy*, Cambridge 2015, https://doi.org/10.1017/CBO9781139198325.

Bērziņa I. "From 'Total' to 'Comprehensive' National Defence: The Development of the Concept in Europe", *Journal on Baltic Security*, vol. 6, no. 2 (2020), pp. 1-9.

Bousquet A.J., *The Eye of War: Military Perception from the Telescope to the Drone*, Minneapolis 2018, https://doi.org/10.5749/j.ctv6hp332.

Cantwell J., Hayashi T. (eds), *Paradigm Shift in Technologies and Innovation Systems*, Cham 2019, https://doi.org/10.1007/978-981-32-9350-2.

Chamayou G., *A Theory of the Drone*, transl. by J. Lloyd, New York 2015.

Cudworth E., Hobden S., "Beyond Environmental Security: Complex Systems, Multiple Inequalities and Environmental Risks", *Environmental Politics*, vol. 20, no. 1 (2011), pp. 42-59, https://doi.org/10.1080/09644016.2011.538165.

Driver D., "The European Union and the Comprehensive Civil-Military Approach in Euro-Atlantic Security: Matching Reality to Rhetoric", *Strategic Studies Quarterly*, vol. 4, no. 3 (2010), pp. 136-155.

Elias N., "Technization and Civilization", *Theory, Culture & Society*, vol. 12, no. 3 (1995), pp. 7-42, https://doi.org/10.1177/026327695012003002.

Enemark Ch., *Armed Drones and the Ethics of War: Military Virtue in a Post-Heroic Age*, London 2014, https://doi.org/10.4324/9780203107218.

Fagan M., "Security in the Anthropocene: Environment, Ecology, Escape", *European Journal of International Relations*, vol. 23, no. 2 (2017), pp. 292-314, https://doi.org/10.1177/1354066116639738.

Fuerst-Bjeliš B., Leimgruber W. (eds), *Globalization, Marginalization and Conflict: Political, Economic and Social Processes*, Cham 2020, https://doi.org/10.1007/978-3-030-53218-5.

Heim M., *The Metaphysics of Virtual Reality*, New York 1993, https://doi.org/10.1093/acprof:oso/9780195092585.001.0001.

Himes K.R., *Drones and the Ethics of Targeted Killing*, Lanham, MD 2016.

Holmes D., "Introduction: Virtual Politics – Identity and Community in Cyberspace", in D. Holmes (ed.), *Virtual Politics: Identity and Community in Cyberspace*, London 1997.

Jones S.G. (ed.), *CyberSociety: Computer-Mediated Communication and Community*, London 1995.

Kamieński Ł., *Mimowolne cyborgi. Mózg i wojna przyszłości*, Wołowiec 2022.

Krelina M., "Quantum Technology for Military Applications", *EPJ Quantum Technology*, vol. 8 (2021), art. 24, https://doi.org/10.1140/epjqt/s40507-021-00113-y.

Lawson S., Middleton M.K., "Cyber Pearl Harbor: Analogy, Fear, and the Framing of Cyber Security Threats in the United States, 1991-2016", *First Monday*, vol. 24, no. 3-4 (2019), https://doi.org/10.5210/fm.v24i3.9623.

Major C., Mölling Ch., "More Than Wishful Thinking? The EU, UN, NATO and the Comprehensive Approach to Military Crisis Management", *Studia Diplomatica*, vol. 62, no. 3 (2009), pp. 21-28.

Malakooti B., "Decision Making Process: Typology, Intelligence, and Optimization", *Journal of Intelligent Manufacturing*, vol. 23, no. 3 (2012), pp. 733-746, https://doi.org/10.1007/s10845-010-0424-1.

Margolis M., Resnick D., *Politics as Usual: The Cyberspace 'Revolution'*, London–Thousand Oaks–New Delhi 2000.

Masys A.J. (ed.), *Security by Design: Innovative Perspectives on Complex Problems*, Cham 2018, https://doi.org/10.1007/978-3-319-78021-4.

Mazarr M.J., *Unmodern Men in the Modern World: Radical Islam, Terrorism, and the War on Modernity*, Cambridge 2007.

McGonagle J.J., Vella C.M., *Proactive Intelligence: The Successful Executive's Guide to Intelligence*, London 2012, https://doi.org/10.1007/978-1-4471-2742-0.

Mérand F., Hofmann S.C., Irondelle B., "Governance and State Power: A Network Analysis of European Security", *Journal of Common Market Studies*, vol. 49, no. 1 (2011), pp. 121-147, https://doi.org/10.1111/j.1468-5965.2010.02132.x.

Miller G., Belton C., "Russia's Spies Misread Ukraine and Misled Kremlin as War Loomed", *The Washington Post*, 19 August 2022, at https://archive.ph/97QJv.

Panteli N., Chiasson M. (eds), *Exploring Virtuality within and beyond Organizations: Social, Global and Local Dimensions*, Basingstoke 2008, https://doi.org/10.1057/9780230593978.

Rid T., "Cyber War Will Not Take Place", *Journal of Strategic Studies*, vol. 35, no. 1 (2012), pp. 5-32, https://doi.org/10.1080/01402390.2011.608939.

Rossiter A. (ed.), *Robotics, Autonomous Systems and Contemporary International Security*, London–New York 2021, https://doi.org/10.4324/9781003109150.

Sarker I.H., Furhad M.H., Nowrozy R., "AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions", *SN Computer Science*, vol. 2 (2021), art. 173, https://doi.org/10.1007/s42979-021-00557-0.

Sayler K.M., "Emerging Military Technologies: Background and Issues for Congress", Congressional Research Service, 6 April 2022, at https://sgp.fas.org/crs/natsec/R46458.pdf.

Scharre P., *Army of None: Autonomous Weapons and the Future of War*, New York 2018.

Singer P.W., *Wired for War: The Robotics Revolution and Conflict in the 21st Century*, New York 2009.

Sloggett D., *Drone Warfare: The Development of Unmanned Aerial Conflict*, Barnsley 2014.

Sonne P. et al., "Battle for Kyiv: Ukrainian Valor, Russian Blunders Combined to Save the Capital", *The Washington Post*, 24 August 2022, at https://www.washingtonpost.com/national-security/interactive/2022/kyiv-battle-ukraine-survival/?itid=na_top_nav.

Stein G.J., "Total Defense: A Comparative Overview of the Security. Policies of Switzerland and Austria", *Defense Analysis*, vol. 6, no. 1 (1990), pp. 17-33, https://doi.org/10.1080/07430179008405428.

Stępka M., *Identifying Security Logics in the EU Policy Discourse: The 'Migration Crisis' and the EU*, Cham 2022, https://doi.org/10.1007/978-3-030-93035-6.

Stone J., "Cyber War *Will* Take Place!", *Journal of Strategic Studies*, vol. 36, no. 1 (2013), pp. 101-108, https://doi.org/10.1080/01402390.2012.730485.

Straub J., "Defining, Evaluating, Preparing for and Responding to a Cyber Pearl Harbor", Technology in Society, vol. 65 (2021), 101599, https://doi.org/10.1016/j.techsoc.2021.101599.

Szerszynski B., "The End of the End of Nature: The Anthropocene and the Fate of the Human", *The Oxford Literary Review*, vol. 34, no. 2 (2012), pp. 165-184, https://doi.org/10.3366/olr.2012.0040.

Turner H.Ch., "Cyber War Forthcoming: »It Is Not a Matter of If, It Is a Matter of When«", E-International Relations, 8 July 2020, at https://www.e-ir.info/2020/07/08/cyber-war-forthcoming-it-is-not-a-matter-of-if-it-is-a-matter-of-when/.

Vestby A., Vestby J., "Machine Learning and the Police: Asking the Right Questions", *Policing. A Journal of Policy and Practice*, vol. 15, no. 1 (2019), pp. 44-58, https://doi.org/10.1093/police/paz035.

Vincze E, Bartha A., Virág T., "Theoretical Potential of Addressing Production of Marginality at the Crossroads of Spatial Exclusion and Development", *Intersections: East European Journal of Society and Politics*, vol. 1, no. 4 (2015), pp. 4-13, https://doi.org/10.17356/ieejsp.v1i4.174.

Wither J.K., "Back to the Future? Nordic Total Defence Concepts", *Defence Studies*, vol. 20, no. 1 (2020), pp. 61-81, https://doi.org/10.1080/14702436.2020.1718498.

Artur GRUSZCZAK is a Professor of Social Sciences, Chair of National Security at the Faculty of International and Political Studies, Jagiellonian University in Kraków, Poland. He is an expert of the Centre International de Formation Européenne in Nice. He has provided expertise in security and intelligence matters for the Polish Ministry for Foreign Affairs, the Polish Parliament, the Polish Ombudsman, the European Parliament and independent analytical institutions such as Statewatch, Oxford Analytica and GLOBSEC. He is the author of *Intelligence Security in the European Union. Building a Strategic Intelligence Community* (Palgrave Macmillan, 2016). He is the co-editor of the *Routledge Handbook of the Future of Warfare* (Routledge, forthcoming 2023). His current research interests include European intelligence cooperation, democratic security and security protocolarization.

Mateusz KOLASZYŃSKI, Ph.D., lawyer and political scientist, is an Assistant Professor at the Chair of National Security at the Faculty of International and Political Studies, Jagiellonian University in Kraków, Poland. His research interests include intelligence oversight in democratic states and surveillance studies. He is the principal investigator in the research project *The influence of the Constitutional Court on the legal framework for intelligence oversight in Poland*, financed by the National Science Centre (grant no. 2021/43/D/HS5/02958).