sciendo

Land Forces Academy Review
Vol. XXVI, No. 4(104), 2021

THE IMPACT OF EMERGING AND DISRUPTIVE TECHNOLOGIES ON SECURITY

Ion OPRIȘOR
Presidential Administration of Romania

ABSTRACT

Emerging and disruptive technologies have mostly beneficial effects, determining the progress of society and rising the standard of living. Their integration in the subsequent strategies in the fields of economy, financial, energy, defence and security, information etc. can generate positive effects for the society as a whole. On the other hand, the malicious use of new technologies will amplify the risks and threats that a technological advanced state can project on other states or an alliance. As a result, new technologies bring human development opportunities as well as challenges and security risks. Therefore, the role of the state becomes essential not only from the perspective of supporting technological innovation, but also from that of managing security risks arising from emerging areas. With regard to Romania, our country is aware of the importance of developing emerging and disruptive technologies in all domains of social life, in particular in the sectors of economy and security and defence. To address the malicious use of emerging and disruptive technologies, Romania aims at adopting complex measures based on an inter-institutional approach to enhance national resilience in domains that new technologies can affect the human activity.

KEYWORDS: emerging and disruptive technologies, security and defence, resilience

Lately, the technological field has seen a great progress, which has led to major changes in the way of life of individuals, the functioning of society and even the repositioning of some states within the international relations system.

Nowadays, there are more and more debates about the development of revolutionary technologies with disruptive effects. However, this kind of changes occurred during every evolutionary stage of the individual and human society, revolutionizing the technologies and the evolution of human society to a new and higher level of development.

Emerging and disruptive technologies are improved or completely new technologies, capable of generating radical changes in some areas of human activity. Essentially, these technologies have mostly beneficial effects in determining the progress of society and rising the standard of living. The implementation of emerging and disruptive technologies requires the change of an important part of the philosophy of human society's functioning, as well as of the relations between individuals and even of the relations between states.

Integration of emerging and disruptive technologies in subsequent strategies in the fields of economy, finance, energy, defence and security, information etc. can generate positive effects for the society as a whole.

On the other hand, emerging and disruptive technologies can be used in various ways that can affect the security of

DOI: 10.2478/raft-2021-0033
© 2017. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 License.

the individuals and society, as well as the military domain. In this context, the new technologies will catalyse the risks and threats that a technological advanced state can project on other states or on an alliance.

As a result, new technologies, some of them emerging and disruptive, bear both development opportunities, and challenges and security risks to human society.

The risks concern individuals, with the possibility of affecting their rights and freedoms, and the society as a whole, as well as the security architecture at regional and global level and even the international order.

In this context, making aware the state authorities to the potential of emerging and disruptive technologies becomes imperative to achieve sustainable development goals, respectively to effectively address new economic, social and environmental realities.

The lack of full understanding of the possibilities of emerging and disruptive technologies and the vulnerabilities that can be exploited is likely to lead to serious consequences for national security and defence. The risks can range from collecting/extracting sensitive data and information about the organization and the functioning of a state' security system to compromising elements of critical infrastructure in key areas of social life, including those of critical importance for national security.

Currently, more and more states have noticed the importance of the connection to the process of research, development and implementation of new technologies, being aware that the technological gap can be a significant vulnerability, including in terms of national security. As a result, *"some countries have already embarked on a global race for supremacy in the field of new technologies, developing dedicated policies and strategies and making significant investments in research and development of disruptive technologies [...]"* (Iancu, 2019).

This aspect is increasingly relevant, as the innovative factor becomes more and more an essential indicator of the power and relevance of a state in the international relations equation, influencing its defence capacity. Thus, the general competitiveness and efficiency of the national interests' management directly relate to the speed of adaptation to technological developments, and the capacity of transformation in accordance with the rigors of the information age and to the response to specific challenges.

"Regardless of the perspective, the effects of technological developments on human society will be vast. Major transformations are already taking place, and the security issues they raise are growing. Therefore, the binomial between technology and security offers the semasiology prevalent in the strategic and political debates of the present. The techno-geopolitics of the high-tech world, in which states and individuals interact in a completely different way than they have done in the past, offers topics that overrun the security agendas with precious language and abstract themes. Most major national and global security analysis and forecasting platforms consider the disruptive technologies as the greatest contemporary challenges facing humanity" (Iancu, 2019).

The rapid evolution of emerging and disruptive technologies and their considerable impact on everyday life raise a series of issues regarding the role of individual in the new social, economic and political architecture, based on digitalization.

Under these conditions, the role of the state becomes essential not only from the perspective of supporting technological innovation, but also from that of managing security risks arising from these emerging areas. Emerging and disruptive technologies generate effects and prospects for use in the military domain, the mass destruction weapons and their vectors of proliferation, cybercrime, organized crime,

activities related to terrorism, extremism and radicalization.

According to the *NATO Science & Technology Organization* (2020) *"the emerging technologies are those technologies or scientific discoveries expected to reach maturity in the period of 2020-2040, that are not widely in use currently or whose effects on Alliance defence, security and enterprise functions are not entirely clear"*.

The term "technology convergence" is also used. It defines the act of combination of some technologies in a novel manner in order to create a synergistic disruptive effect.

Given the special importance that emerging and disruptive technologies will have on security, documents of this year's NATO Summit reflect this evolution. According to NATO documents, the speed of technological change has never been faster creating opportunities and risks in the security environment as well as in the way the Alliance operates.

"We are determined to preserve our technological edge, and ensure Alliance interoperability, in order to maintain the credibility of our deterrence and defence posture. We have recently taken important steps to that end, building on the Emerging and Disruptive Technologies Roadmap we agreed in 2019, and have now adopted our strategy to foster and protect EDTs. This strategy outlines a clear approach for identifying, developing, and adopting EDTs at the speed of relevance, guided by principles of responsible use, in accordance with international law, and taking into account discussions in relevant international fora" (NATO, 2021).

Considering the pace and scale of the technological developments, it is necessary that, along with the development of security forces and capabilities, NATO and the European Union as organizations as well as the Member States to recognize the vital importance of research and innovation in order to explore opportunities and meet the challenges generated by the emerging and disruptive technologies. This will lead to keeping the current technological edge of NATO and its members.

At the same time, by launching the civil-military *Defence Innovation Accelerator for the North Atlantic Area* and by setting up a *NATO Innovation Fund*, the interested Allies could contribute to supporting new activities in emerging and disruptive, as well as dual-use technologies domains, in key areas for the Allied security.

The use of emerging technologies in the fight against terrorism is also considered.

Significant efforts are also underway at the European Union's level in order to maintain the technological edge and support the European industrial base. Thus, *EU's Multiannual Financial Framework for 2021-2027* envisages a significant increase of investment in the defence technologies as well as in the related civilian areas, such as security, mobility, health, information management, cybernetics and space.

In the European Union's assessment, *"the term disruptive technology refers to a technology inducing a disruption or a paradigm shift, i.e. a radical rather than an incremental change. Development of such a technology is high risk, high potential impact, and the concept applies equally to the civil, defence and space sectors. Disruptive technologies for defence can be based on concepts or ideas originating from non-traditional defence actors and find their origins in spin-ins from the civil domain"* (European Commission, 2021, p. 13).

An important part of the *Digital Europe Program* will support disruptive technologies for civil applications. Other EU funding instruments, including those of the *Space Programme*, envisage similar investments.

In order to foster innovation and ensure the competitiveness of EU industry,

an ambitious skills policy is also necessary to identify possible shortages and potential for synergies in the interaction between the civil, defence and the spatial domains.

In this context, the European Commission intention to launch an "innovation incubator" to support new technologies and shape dual-use innovation, in cooperation with the *European Innovation Council* and other stakeholders, in the first half of 2022 is timely and useful. The Commission will also support cross-border defence innovation networks that will test the relevance of technologies in the civil sector and support responsible innovation in defence value chains (European Commission, 2021, pp. 13-14).

In the military field, emerging and disruptive technologies provide significant benefits to developing countries, with the effect of reconfiguring military capabilities, but also the physiognomy of a potential conflict. In this context, some countries are already carrying out concrete projects for the implementation of new technologies, which will have special implications for the global security.

Consequently, it is essential for the states and international organizations they are part of to support research projects and the exploitation of scientific potential, to set regulation of emerging fields, and to guarantee the right to privacy and personal data. This is one of the main arguments for the states and the international bodies they are part of to act together, based on coherent strategies to adopt new technologies, to strengthen the industrial sector and maintain the technological edge. A coherent strategy should be based on the combined effort of the public authorities, public-private partners, academia and society as a whole.

Foreshadowing an imminent change in military standards, many states and organizations are investing heavily in developing optimal solutions for the implementation of emerging and disruptive technologies in the area of offensive and defensive capabilities.

The development of technologies based on Artificial Intelligence must transform and improve military activities, especially components of intelligence, image recognition, video surveillance, autonomous systems, cyber operations, logistics and human resources, disinformation operations, analysis of risk, command and control, etc.

Artificial Intelligence can also have significant impact on the proliferation of weapons due to the possibility of assimilation into a technology or product, which cannot be immediately detected and controlled.

At the same time, it is necessary to modernize the current mechanisms for control and verification of relevant weapons and military activities and to increase trust between states, such as through the *Vienna Document 2011*, to return, refine and update formats or treaties, e.g. the *Intermediate-Range Nuclear Forces Treaty* and *Open Skies Treaty*.

These mechanisms would ensure an increased predictability in the regional and global security architecture building, would improve stability, making funds available for other sectors of human activity (such as health, education, infrastructure etc.). Last, but not least, it would avoid an arms race which could have unpredictable effects in the future, given the current technological progress.

In this context, states that possess or develop emerging and disruptive technologies with a high destructive effects, particularly in the production, testing and operationalization of new weapon systems (such as hypersonic weapons, high power lasers, directed energy systems etc.) should accept the control and verification mechanisms and should contribute to their improvement and increased efficiency. Such a behaviour would benefit the global security.

Another significant challenge is the ability of some actors or entities (states, organizations, individuals, groups etc.) to access new technologies. Easy access to technology facilitates some entities or individuals to conduct research and technological activities that are beyond the control of states and outside the legal commercial framework. Moreover, while some states have to comply with the internationally agreed norms and standards, other state or non-state actors will circumvent these rules.

With regard to Romania, our country is aware of the importance of developing emerging and disruptive technologies in all areas of social life, especially in the sectors of economy and security and defence, and aims at supporting both basic and applied scientific research, particularly in the economic environment.

Only by combining the performances of both systems, our country will position itself on an upward path in the development and implementation of the emerging and disruptive technologies for the benefit of our society and individuals.

As for the protection against the malicious use of emerging and disruptive technologies, Romania aims at adopting complex measures in a whole of government approach to increase resilience at all the levels that new technologies could affect human activity.

In this context, establishing the *Euro-Atlantic Centre for Resilience* in Bucharest is part of our country's effort in this direction.

Of course, the *Centre* is in its early-stage of functioning at present. However, after its full operationalization, a process that is desirable to involve as many NATO, EU and partner states as possible, we will have an effective tool that will contribute to maintaining and increasing resilience, to include effects generated by the malicious applicability of emerging and disruptive technologies.

Particularly important will be the collaboration of the *Centre* with the private sector, academia, international research institutions and civil society to facilitate the development of a societal resilience approach.

It will also provide a platform for strategic discussions and development of concepts, training and exercises, as well as for the collection and delivery of lessons learned and will allow the development of various resilience programs and initiatives.

During the next period, the activity of the *Centre* will focus on the following topics:

- Societal resilience;
- Resilience in the field of emerging and disruptive technologies;
- Resilience of communication systems, ecosystems and novel technologies;
- Resilience to crises and complex emergencies;
- Ensuring continuity of government and critical services;
- Resilience of transport infrastructure;
- Resilience of neighbour states of NATO and EU to anti-Western influence performed by state and non-state actors.

At the same time, Romania adapts its programmatic documents to the new security challenges and technological evolutions with impact in the field of security and defence. Thus, *The National Defence Strategy for the period of 2020-2024*, and *The White Paper on Defence and The Military Strategy of Romania* include references to emerging and disruptive technologies along with information manipulation, political coercion, attempts to create satellite states, challenges to representative democracy, and unprecedented development of military capabilities. Actors challenging the current world order regard all these as tools for action.

According to these documents, within the military procurement programs, the Romanian Armed Forces will pursue,

among others, the acquisition of weapon systems and equipment based on innovative, emerging and disruptive technologies as well as the development of techniques, tactics and procedures for their use in operations.

Summarizing, it can be assessed that the ongoing new technological revolution will contribute to the transition of human society to a new level of progress, will bring major opportunities but, at the same time, significant security challenges.

In this context, states need to collaborate and coordinate their efforts bilaterally, multilaterally and within the alliances and organizations they are part of in exploiting the opportunities and, especially, in managing the security challenges.

At the same time, there is a need for a comprehensive process to adapt the national security systems, increase the role of the whole of government approach to reduce vulnerabilities, modernize and transform international organizations. Both NATO and EU have initiated such a process to address the need to adapt to the new international security environment.

To achieve this goal, the legal framework has to be reviewed and adapted to the new technological and security realities, in order to optimize the synergy between the national institutions with relevance in the security field, on one hand, and between the states within the security organizations, on the other hand. Adapted rules, procedures and strategies will be required in this effort.

Given the dynamics and pace of development in emerging and disruptive technologies, it is imperative for all public institutions with responsibilities in the security and defence domain to assign intelligence and managerial resources to study, analyse and set concrete objectives to identify and eliminate vulnerabilities generated by this new field.

The academic environment has to implement in the study programs, both theoretical and practical-applicative ones, especially the latter, elements specific to emerging and disruptive technologies so that the university curricula to be permanently updated in line with the new worldwide technological development. Practical applications must capitalize on these theoretical developments and accustom students to operationalize their knowledge in a competitive environment specific to emerging and disruptive technologies.

Fundamental and applied scientific research in Romania has to pay special attention to these new technologies, the implications they generate at the level of Romanian society, emphasizing those in the economic and national security fields.

The security culture in Romania, resulting from the convergent actions of public institutions, academia, and security think tanks has to impact both national relevant actors and citizens, so that all of them to be aware of the emerging and disruptive technologies' importance. Thus, we can manage the development of scientific and technological knowledge of the nation, and counter the security challenges.

Against this background, Romania has to be active within the international framework, primarily in NATO and the European Union, as well as in the UN and OSCE. Our country should have a constructive position, promoting effective management of risks and threats associated with the malicious use of emerging and disruptive technology by appropriate and proactive actions.

REFERENCES

European Commission. (2021). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Empty*, 13.

Iancu, N. (2019). *Tehno-geopolitica securității globale și autocrația digitală în epoca inteligenței artificiale*. Available at: https://monitorulapararii.ro/tehno-geopolitica-securitatii-globale-si-autocratia-digitala-in-epoca-inteligentei-artificiale-1-24865, accessed on 07 July 2021.

NATO Science & Technology Organization. (2020). *Science & Technology Trends 2020-2040 Exploring the S&T Edge*. p. 6.

North Atlantic Treaty Organization (NATO). (2021). *Brussels Summit Communiqué*. paragraph 37.

BIBLIOGRAPHY

Congressional Research Service. (2021). *Emerging Military Technologies: Background and Issues for Congress*. Available at: https://crsreports.congress.gov/product/details?prodcode=R46458.

Cummings, M.L. (2017). *Artificial Intelligence and the Future of Warfare*. Chatham House, available at: https://www.chathamhouse.org/sites/default/files/publications/ research/2017-01-26-artificial-intelligence-futurewarfare-cummings-final.pdf.

Defence White Paper. (n.d.). Available at: https://sgg.gov.ro/1/wp-content/uploads/2021/03/ CARTA-ALBA-A-APARARII-.pdf.

European Commission. (2021). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Empty*. *Action Plan on synergies between civil, defence and space industries.* Available at: https://ec.europa.eu/info/sites/default/files/ action_plan_on_synergies_en.pdf.

Fitzgerald, B., & Sayler, K. (2014). *Creative Disruption Technology, Strategy and the Future of the Global Defense Industry*. Available at: https://www.leonardodrs.com/media/1202/cnasfutureoftheglobaldefeseindustry.pdf.

Iancu, N. (2019). *Tehno-geopolitica securității globale și autocrația digitală în epoca inteligenței artificiale*. Available at: https://monitorulapararii.ro/tehno-geopolitica-securitatii-globale-si-autocratia-digitala-in-epoca-inteligentei-artificiale-1-24865.

Koutroumpis, P., & Lafond, F. (2020). *Disruptive technologies and regional innovation policy*. Available at: https://ik.org.pl/wp-content/uploads/geopolitics-of-emerging-and-disruptive-technologies-2020.pdf.

National Defence Strategy 2020-2024. Available at: https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf.

NATO Advisory Group on Emerging and Disruptive Technologies. (2020). *Annual Report 2020*. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/210303-EDT-adv-grp-annual-report-2020.pdf.

NATO Science & Technology Organization. (2020). *Science & Technology Trends 2020-2040 Exploring the S&T Edge*. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.

North Atlantic Treaty Organization (NATO). (2021). *Brussels Summit Communiqué*. paragraph 37. Available at: https://www.nato.int/cps/en/natohq/news_185000.htm.

Raska, M. (n.d.). *Strategic Competition for Emerging Military Technologies Comparative Paths and Patterns*. Available at: https://ndupress.ndu.edu/Portals/68/Documents/ prism/prism_8-3/prism_8-_Raska_64-81.pdf.

Rekowski, M., Piekarz, T., Sztokfisz, B., Siudak, R., Albrycht, I., Roguski, P., Kostkiewicz, P., Siciarek, M., Silicki, K., Wrzosek, M., Dylik, T., Buchner, T., Świątkowska, J., Rodríguez, A., & Mikulski, K. (2020). *Geopolitics of emerging and disruptive technologies*. Available at: https://ik.org.pl/wp-content/uploads/geopolitics-of-emerging-and-disruptive-technologies-2020.pdf.

Romanian Military Strategy. (2020). Available at: https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf.

Yanakiev, Y., Stoianov, N., Kirkov, D., & Velev, G. (n.d.). *Defence Strategy and New Disruptive Technologies Nexus: Implications for the Military Organisations*. Available at: https://www.di.mod.bg/.

Zegart, A., & Childs, K. (2018). *The Divide between Silicon Valley and Washington Is a National-Security Threat*. Available at: https://www.theatlantic.com/ideas/archive/2018/12/growing-gulf-between-siliconvalley-and-washington/577963/.