EMERGING AND DISRUPTIVE TECHNOLOGIES' IMPACT ON THE MILITARY

Colonel Sorinel POPESCU
Ministry of National Defence

The article addresses the emerging and disruptive technologies domain, highlighting that they will provide opportunities for the development of society and security challenges, as well. In this context, national and international security systems need to adapt and go through an extensive process of transformation, allowing them to mitigate the effects generated by the implementation of new technologies both in the civilian field, but especially in the military. Subsequently, the development of new technologies will lead to a new revolution in the military, which will change the physiognomy of the armed conflict. Starting from these premises, the article identifies elements related to the impact that new technologies will have on planning and conducting an armed conflict, but also some opportunities and challenges to the military as a whole. The article concludes that emerging and disruptive technologies will have a decisive contribution in the human society's transition to a higher level of development, but their malicious use will be one of the major challenges facing national authorities and international security organisations.

In the development of the article, I used as study methods the documentation and qualitative analysis of some bibliographic materials that address the field of emerging and disruptive technologies.

Keywords: emerging and disruptive technologies; security and defence; security challenges; physiognomy of military conflict;

INTRODUCTION

Humankind is in a preliminary stage of unprecedented technological development. Probably, the current period is preparing/making the transition to a large magnitude technological era that will revolutionise the functioning of human society and the way in which the individual will relate to the new type of society. At this time, it is difficult to predict the way of life/human behaviour in a few decades, if the technological revolution, foreseeable for the coming years, is successful.

Since its inception, human society has been in a perpetual evolution. The main catalyst for the transition of society from a lower level of development to a higher one has been the human aspiration to expand knowledge of the environment, increase living standards and improve the existing technical tools, which allow the expansion and a better life. The way in which human society has managed to evolve is based on the technological innovation materialised in the development and implementation of new technologies, characteristic of each historical period, part of them having, at the particular time, disruptive effects.

Over time, emerging and disruptive technologies have been developed and implemented mainly in the military field (the explosive, the aircraft, tracked armoured vehicle, the missiles developed by Germany in the Second World War, the nuclear energy, the INTERNET network etc.), later being taken over by civilian industry segments. In recent years, there has been a reverse trend, the continued transference of the centre of gravity of the technologies' development from the military to the civilian sphere, the development of new technologies being the result of major investments in commercial sectors. Emerging and disruptive technologies have particularly beneficial effects, determining the progress of society and increasing the standard of living of the individual. Their implementation in the civil fields of human activity can generate positive effects in the economy and society.

According to *NATO Agency for Science and Technology*, *"emerging technologies are those technologies or scientific discoveries that are expected to reach maturity in the period 2020-2040; and, are not widely in use currently or whose effects on Alliance defence, security and enterprise functions are not entirely clear. Disruptive technologies are those technologies or scientific discoveries that are expected to have a major, or perhaps revolutionary, effect on NATO defence, security or enterprise*

functions in the period 2020-2040". (NATO Science & Technology Organization, p. 6). At the same time, the term *"technology convergence"* is also presented in the aforementioned document, which represents the action of combining the effects of new technologies in an innovative way in order to create a synergistic disruptive effect.

According to NATO, *data, artificial intelligence, autonomous systems, space systems, hypersonic systems* are seen to be predominately disruptive in nature, while developments in the fields of *quantum*, *biotechnology* and new types of *materials* are considered emerging and requiring a longer time until their disruptive effect will have a high impact on the military. Most likely, the disruptive effects will appear as a result of the synergy of different technical fields: *data-artificial intelligence-autonomous systems*; *data-artificial intelligence-biotechnology*; *space systems-hypersonic systems-materials* etc.

Security, transparency, impartiality, ethical principles and fundamental human rights must guide the process of adopting new technologies, in order to avoid altering their original purposes and reducing security risks. Research, development and implementation of new technologies in the economy, security and defence sectors will lead to widening the gaps that already exist between some states or, why not, to reducing the differences between others. The states that will be the first to develop/ implement viable emerging and disruptive technologies will start with a major advantage, which will catalyse an exponential economic and technological development.

Artificial Intelligence, a basic component of the new technologies, could be the substance of the fourth industrial revolution, a game changer with the potential to influence developments in all sectors – transport, industrial and energy production, health, education, media, public services, security and defence.

On the other hand, the malicious use of new technologies potentiates the risks and threats that a state or non-state actor, which has this technological advance, can project on another state or on an alliance. From this point of view, the implementation of new technologies brings significant challenges to key decision-makers, who must quickly adapt to new trends in society. Under these conditions, the role of state authorities becomes essential both from the perspective of promoting and supporting the process of technological innovation, and from the position of managing the security risks associated with the field of emerging and disruptive technologies.

With regard to the security field, the development of new technologies creates the prerequisites for states that have this capacity to get major advantages over others, being very likely to re-establish international relations and, ultimately, modify or even create new security architectures at regional and global level.

THE IMPACT OF EMERGING AND DISRUPTIVE TECHNOLOGIES ON THE MILITARY

As in other periods of the evolution of human society, the development of new technologies will lead to a revolution in the military field, which will determine a change in the physiognomy of armed conflict. This will require new strategies, and at the tactical level, the development of new techniques, tactics and operational procedures for the use of forces and equipment in operations.

The international competition for development and implementation of new technologies is fierce, with various states and organisations carrying out ambitious investments and projects in the field. As in the civilian field, any delay can lead to the accumulation of a long-term technological gap at the military level, too. In this context, some states have already got a head start, investing heavily and developing new technologies with applicability in the military field. The challenges facing these states are associated with the processes of identifying and creating mechanisms for the integration of emerging and disruptive technologies into advanced military systems, already operational, within the various military branches and specialties.

The issue of emerging and disruptive technologies was also discussed during this year's NATO Summit and reflected in its final documents. According to NATO documents, the current speed of technological change is unprecedented, which creates opportunities and risks for the security environment, as well as for the way in which the Alliance will fulfil its three fundamental tasks: collective defence, crisis management and security through cooperation. *"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 the emerging and disruptive technologies. This strategy outlines a clear approach for identifying, developing, and adopting the emerging and disruptive technologies 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"*.

(*Communiqué of the NATO Summit in Brussels*, 14 June 2021, para. 37). During this Summit, launching the *Civil-Military Accelerator of Innovation in the Defence of the North Atlantic* and the establishment of the *NATO Innovation Fund* were agreed as platforms through which Allies can contribute to supporting actions in emerging and disruptive technologies with dual use domain, in key areas for Allied security.

It is expected that in the next 20 years, advanced technologies in the military field to be based on four predominant fundamental characteristics: intelligent, interconnected, distributed and digital, characteristics that will determine the transition of war to a new generation *(figure no. 1)*. Of course, in this context, we refer to war as a complex social phenomenon, and the new technologies will have applicability on all lines of effort, and not only on the military that is materialised, ultimately, in military conflict.

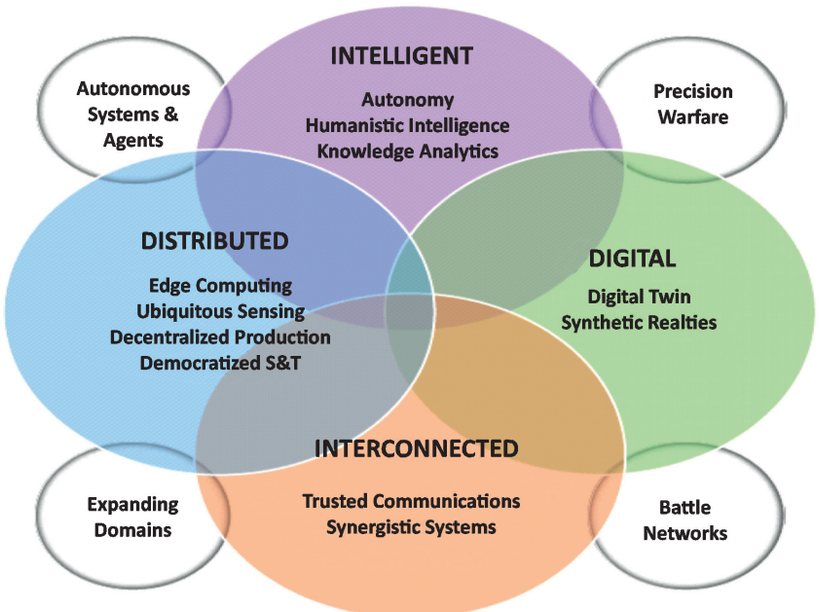

Figure no. 1: Intelligent-Interconnected-Distributed-Digital (I2D2) with associated military trends, NATO Science & Technology Organization, p. 8.

Referring to the line of military effort, the most important effects will be produced in the decision-making process; command and control; surveillance, recognition and early warning; long-range and high-precision striking capabilities; concealment and force protection; deception, increasing the energy storage capacity of striking vectors and weapons platforms etc. (NATO Science & Technology Organization, p. vi-vii).

The synergy of the four characteristics will lead to a change in the physiognomy of the armed conflict. Support and striking systems based on new technologies, especially those using *Artificial Intelligence*, will increase the efficiency of current combat functions and lead to the creation of an enhanced operational and tactical synergy.

Conjugated use of *intelligent and distributed technologies* will facilitate the development of systems/platforms/robots with high autonomy and whose operational possibilities will be clearly superior to human fighters.

The extensive use of *Artificial Intelligence* will allow autonomous systems to support the decision-making process by analysing a very large number of variables and based on multiple criteria. Autonomous agencies/systems will provide rapid analysis, different courses of action in the planning process, generating completely new solutions that are not constrained by the old strategies. At the same time, the systems/platforms/robots with high autonomy will ensure an increased synergy between the human fighter and the personal equipment, increasing the efficiency of military actions. *"The technological process will lead to further integration for such systems. They will become capable of carrying out increasingly more complex tasks in a coordinated manner. The missions they carry out will facilitate the automated acquiring of effective methods, and the lessons they learn will be stored in real-time in a new type of artificial conscience of the concept of operations, in order to be instantaneously transformed into commands, which will impede the enemy from fully adapting to the dynamics of the operational field"* (Iancu, 2019).

The interaction between *interconnected and digital* will lead to creating interconnected combat networks (command and control, reconnaissance and surveillance, delivering fire systems etc.), which will ensure a greater integration of sensors and facilitate the command-and-control process reducing the time of plans and orders' transmission, battle damage assessment etc. On the other hand, these networks will facilitate major operational dependencies between the different command-control structures and integrated armament systems, the networks themselves, being, at the same time, high value targets for the opponent. *"This increased reliance on seamless and ubiquitous connectivity will increase the value in targeting such networks (military or civilian) in disinformation, cyber or physical manner. Such attacks may be implemented long before the conflict itself is initiated, and could strike indirectly at logistic, personnel, information, financial or other supporting elements of modern operational and strategic networks"* (NATO Science & Technology Organization, p. 9).

The effects produced by the synergy between *interconnected and distributed* technologies will lead to extending the operational domains of military actions. As the operational environment expands, including outer space, the cyber environment, the broader information sphere, the need to design, plan and act in a widely dispersed, interconnected and multi-domain manner will become even more critical. The large number of sensors and their wide distribution, the need to perform multi-field missions, as well as the increased processing capabilities built into state-of-the-art networks will require new standards to maintain functional dominance, protection, countermeasures, counter-countermeasures and other secondary functions.

The association of *intelligent and digital* technologies will increase the accuracy and efficiency of military actions. The high degree of digitalisation of networks, miniaturisation, state-of-the-art processing algorithms, combined with lower and lower production costs have led to the development of intelligent, interconnected and distributed systems. These developments contribute significantly to the diversification of high precision and effect-oriented striking capabilities (ground-launched ballistic and cruise missiles, striking vectors based on air and naval platforms, electronic warfare offensive systems etc.). On the other hand, some high-precision striking capabilities with low production costs (e.g., swarms of mini- UAVs), which are easy to obtain, will be important risk factors, while increased digitisation brings with it vulnerabilities that probably cannot be foreseen at this time. The use of sophisticated analytical tools, which capitalise on the increased volume of data, will lead to a better knowledge of the battlespace; the relevant changes can be noticed almost in real time, as well as the development of new operational capabilities.

OPPORTUNITIES AND CHALLENGES RELATED TO THE IMPLEMENTATION OF EMERGING AND DISRUPTIVE TECHNOLOGIES IN THE MILITARY

The implementation of new technologies in the security and defence systems will determine the emergence of new regional and perhaps even global security architectures. States that currently have a lower role in regional security arrangements could play an important one in the design of these security architectures, if they invest and develop new technologies with high relevance in the field of security and defence.

Given the major challenges (unpredictable and increasingly frequent pandemic developments, rapid climate changes, widespread social unrests etc.) that states are currently facing, we assess that the countries will not be able to address by themselves the danger of the proliferation of new military technologies. It is also very possible that, in this context, state authorities should not pay particular attention to the potential effects of the implementation of emerging and disruptive technologies in the military field and the predictability of their malicious use. Under these conditions, a particularly important role belongs to the major military powers and international security organisations/formats (UN, NATO, Arab League, Collective Security Treaty Organisation, Shanghai Cooperation Organisation etc.), which must develop mechanisms to control and verify the development of new technologies.

In fact, most of the weapon systems that will be developed based on emerging and disruptive technologies are not the object of the current arms reduction, control and verification treaties (New START, Vienna Document etc.). In this context, there is a need to adopt new, up-to-date mechanisms not only in the field of production, ownership and use of new technologies, but also to control their exports, based on comprehensive legislation and regulations applicable to current trends. The mechanisms would ensure a high transparency of military activities related to the development/use/international trade of emerging and disruptive military technologies and to an increased trust between states. Moreover, these mechanisms will contribute to predictability and shape an effective security architecture capable to ensure strategic stability and avoid an arms race, which would lead to a global spiral of insecurity.

States can develop new technologies within government programmes subsequent to major procurement programmes, as well as through *proxies* that are not officially under the control of state authorities, but which, in real terms, are funded by them. Some of the weapon systems developed based on new technologies can be used against other states/alliances through other *proxies* (terrorist organisations, secessionist entities, private security companies etc.), whose activity goes beyond the international legal framework and a strictly delimited territory of a state/group of states. These actions will maintain strategic ambiguity and deny the plausibility of an aggressor state in relation with the targeted state, international community and international security organisations/formats.

During a multi-domain conflict/crisis, at least at the regional level, the integration of new technologies in the lines of effort aimed at creating legitimacy, at domestic and international level, for the aggressor state will pose a particular problem.

On the other hand, the aggressor state will try to affect the political decision, the trust/support of the public opinion of the target state for national authorities, the morale of the armed forces etc.

Currently, most of the human, financial and knowledge resources needed to develop emerging and disruptive technologies are not in the possession of states, but of large multinational technology giants. As a result, states will try to attract them in the development of new technologies, which will also create some vulnerabilities for applicant states whose legislation is deficient, including the creation of major dependencies, which, in crisis and conflict, can turn into risks. In this context, we can even speak about *"a transfer"* of a part of national sovereignty to multinational technology giants.

Another major challenge is the particularly easy access that some third parties may have to emerging and disruptive technologies. The various components, technologies, algorithms etc., can be procured by non-state actors, separately, in parts, later integrated and optimised in systems, an activity that exceeds the control of state and supranational authorities. Using them against elements of civilian infrastructure or IT infrastructure could lead to serious economic, financial and security damages.

The development of emerging and disruptive technologies will increase the role of strategic deterrence to the detriment of effective defence, which is a beneficial element. The new technologies will also facilitate the states that do not currently have nuclear weapons to get a credible deterrent posture, comparable to nuclear powers.

Although nuclear arsenal is currently the main tool of deterrence at the strategic level, with the development of new technologies its relevance will decrease, being replaced by other combat systems that could be possessed by non-nuclear powers, as well. Consequently, it will also be necessary to change/modernise the current international security organisations/global security formats, or even to create new ones in order to maintain a balance between the deterrence and defence posture, on the one hand, and the challenges/threats/ security risks, on the other hand.

As technologies based on *Artificial Intelligence* develop, it is predictable that military actions will have a high level of computerisation. The technical means based on *Artificial Intelligence* will be used in extending the capacities to collect and process battlespace intelligence; image recognition and target surveillance; deception and disinformation; risk analysis; improving the command and control and operational

planning. They will influence the force package tailoring process and their involvement in operations and facilitate complex possibilities of actions.

Due to the self-learning function, the new systems that will support the decision-making process will have the ability to adapt to the dynamics of the theatre of operations, being able to make decisions on their own in a short time. In this context, the synergy level between the human factor (staffs, commanders) and the technical one will be very important. In addition, even if the targeting process will have a high degree of automatization, it will be very laborious and could raise major challenges regarding targets' discrimination, other than technical/physical ones, the time and priority of their engagement etc.

New technologies will also have a high impact on deception activities. Having the ability to duplicate completely the real weapon systems, the dummies will greatly complicate the targeting process at a tactical and operational level. The new dummies will have the ability to adapt to the characteristics of the terrain, weather conditions and time they are under surveillance, but also to the technical possibilities of adverse sensors performing monitoring, sending technical hints of similarity with the real means imitated.

An important benefit that the new analysis and simulation tools will bring into the operational planning process, especially at the tactical and operational levels, is during the war games. The virtual simulation/*digital twin* of reality will allow staffs and commanders to preview the planned actions, choose the optimal courses of action, create branch plans and, ultimately, avoid being surprised while conducting combat actions.

The intensive use of propaganda by one of the belligerents, by creating virtual realities that seriously/completely distort reality, will significantly affect the opponent's morale of troops and public opinion, creating major advantages for the part that uses these means. Thus, effective mechanisms are needed to counteract and manage the effects of these actions. It is important because more and more states are setting up and preparing specialised structures on this segment of action.

The development of weapon systems based on new technologies and their integration in operational environments, so far less used (space, cyber and submarine environments), will lead to a drastic decrease/loss of importance of the spatial dimension of the military conflict, which will determine major changes in the physiognomy of the armed conflict. Many of the current forms of manoeuvre or methods of fighting will disappear.

Another significant challenge, which will affect the way states act in a multinational context or within alliances, NATO included, will be the possibility that some financially and technologically powerful allied states can develop rapidly combat systems and techniques, tactics and procedures based on the new technologies. On the other hand, other countries will not be able to maintain this procurement pace, widening their existing technical gap, which will affect the interoperability of forces and technical means in operations. Therefore, a coherent strategy at the level of alliances to maintain technological advantage and interoperability is required.

CONCLUSIONS

Emerging and disruptive technologies will decisively contribute to the transition of human society to a higher level of development. More and more, human activity will be replaced by operations performed by systems/platforms/robots with high autonomy. New technologies will generate not only opportunities but also security risks. In this context, national/supranational authorities need to adapt quickly to new technological developments and create the legal and actionable framework to optimise the implementation of these technologies for the benefit of society and risk reduction, up to making them manageable.

The technological revolution predicted for the coming years will also determine a new revolution in the military. Providing the forces belonging to the security and defence systems with new generation equipment will require the adaptation/development of the conceptual and actional framework in the new operations. National security strategies, defence white papers and military strategies will be rewritten. The physiognomy of the military conflict will change, leading to the development of new combat manuals, techniques, tactics and procedures for the use of forces and equipment in operations.

Given the struggle to redefine security architectures, in conjunction with the assertiveness of some emerging powers with global recognition aspirations, war, as a social phenomenon, remains omnipresent. The possibility of waging an armed conflict will decrease, but the military potential of a state/alliance, based on next-generation technical combat systems, will support the actions and ensure *"the freedom of movement"* on the other lines of effort: economic, financial, social, informational etc.

The malicious use of new technologies, by both state and non-state actors, will be one of the major challenges facing the national authorities and the leadership structures of various alliances or international security formats. Most states

will not be able to cope with some of the new security challenges alone. It is thus necessary to address them in a multinational, allied context.

The main challenge for NATO will remain to maintain the technological advantage and ensure a high interoperability of multinational forces during the planning process and execution of military operations. The unitary implementation of emerging and disruptive technologies in the military systems of allied states remains the main imperative for an increased interoperability at the Allied level.

At the same time, the cooperation between the civilian and military sectors in the field of technical research will be of special importance. At conceptual level, the involvement of centres for policy and security analysis, think tanks, academia etc. in the process of analysis and identification of the new security challenges and in the ways to address them is more than desirable.

BIBLIOGRAPHY:

1. Iancu, N. (2019). *Noul dicţionar al apărării: tehnologiile disruptive*, https://monitorulapararii.ro/noul-dictionar-al-apararii-tehnologiile-disruptive-1-21024, retrieved on 12 September 2021.
2. *Brussels Summit Communiqué Brussels 14 June 2021*, https://www.nato.int/cps/en/natohq/news_185000.htm, retrieved on 23 September 2021.
3. NATO Science & Technology Organization. *Science & Technology Trends 2020-2040 Exploring the S&T Edge*, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf, retrieved on 12 September 2021.