ANALYSIS OF MULTI-DOMAIN OPERATIONS CONCEPT AND THE ROLE OF EMERGING ADVANCED AND DISRUPTIVE TECHNOLOGIES FOR ITS OPERATIONALISATION

Captain Ionuț-Iulian CĂLUGĂRU, PhD Student
"Carol I" National Defence University, Bucharest

10.55535/RMT.2024.3.5

At present, Multi-Domain Operations (MDO) concept is of interest for the whole defence and security sphere, especially for the Euro-Atlantic area, where its implementation and operationalisation are desired at the level of the military instrument of power, as well as at the national and international strategic level, in an allied and partner context.

The manner in which emerging and disruptive technologies can be transferred and integrated into the military field in order to provide stability and give the concept practical-applicable utility, and the way in which it can be operationalised, are elements of great interest to national military authorities at the moment, while giving the concept a probabilistic character for those analysing this area of the military field.

Moreover, the decision-making process and the operational side are elements that, in the multi-domain integrative framework, require the involvement of advanced technologies, in particular artificial intelligence, which also, as a subdivision of technology, practically marks the existence of the contemporary human being, becoming a basic constituent in the conduct of military actions.

In this article, we will try to give a realistic picture of this concept by presenting information analysed and extracted from bibliographical sources that reflect a qualitative and topical character. Therefore, the research method used throughout this paper will be the bibliographic research method (literature review), through which we will attempt to project a critical analysis of the impact that the concept will have on society.

Keywords: emerging technologies; artificial intelligence; multi-domain operations; decision supremacy; disruptive technologies;

INTRODUCTION

The term *modern battlefield* is used to give a transposition of ideas that are based on empirical elements from the past of armed combat, namely ideas about how military actions can be developed according to human and technological evolution. At the moment, the battlefield picture of the future is shaped around contemporary elements such as *artificial intelligence* and *multi-domain operations* and the way they can be integrated to gain decisional and actional advantage over the adversary. Therefore, the elements mentioned in the previous sentence also substantiate the necessity of the present study, knowing that the time and energy-consuming concern among political and military leaders has always been focused on achieving superiority over the adversary.

The rationale behind this article is the need to understand the impact that artificial intelligence can have at the decision-making level and, even more, at the action level. Technologization is a product of the progress that mankind has made in all spheres of its existence, driven by the desire to dominate in a particular field, practically to take the lead in various competitive areas such as industrial, political, military, economic etc. Disruptive and emerging technologies have occurred as a response to the evolution and development of subsidiary branches of technology such as artificial intelligence, digitalisation, machine learning etc., having a decisive impact on all societal domains, including the military sphere, where the battlespace and, ultimately, the conduct of combat have acquired new facets. Here we refer to the expansion of the battlespace as the physical barrier has been overcome, time has become compressed and the speed of information transmission has increased, making it almost imperceptible, thus creating the conditions for new concepts such as *Multi-Domain Operations (MDO).*

Disruptive and emerging technologies have occurred as a response to the evolution and development of subsidiary branches of technology such as artificial intelligence, digitalisation, machine learning etc., having a decisive impact on all societal domains, including the military sphere, where the battlespace and, ultimately, the conduct of combat have acquired new facets.

The purpose of this study is to provide a clear picture of the way emerging technologies and artificial intelligence, as a subsidiary, are being integrated and used in military operations, particularly in multi-domain operations, and, in more detail, of the decision-making dimension at each of the three levels of military operations: strategic, operational and tactical. The concept of artificial intelligence becoming an essential element of military operations is at this point a goal that is most likely easily achievable. The completeness of the fact that both current and future emerging and disruptive technologies will result in the link between military and non-military aspects, generating, in effect, a new and more complex physiognomy of armed combat, and shaping this integrated multi-domain framework, is of a self-evident character, concretised by the research already in place.

Artificial intelligence can be used to achieve decisional and actional supremacy over the adversary. Starting from this working hypothesis, throughout this article, we will try to highlight those aspects through which artificial intelligence finds its usefulness in the process of military operations and also to understand what the role of the military leader is in this process, considering the characteristics that systems, which are based on this branch of technology, possess.

The hypothesis behind the present study refers to the fact that artificial intelligence can be used to achieve decisional and actional supremacy over the adversary. Starting from this working hypothesis, throughout this article, we will try to highlight those aspects through which artificial intelligence finds its usefulness in the process of military operations and also to understand what the role of the military leader is in this process, considering the characteristics that systems, which are based on this branch of technology, possess.

The most recent and complex studies highlighting the contribution and necessity of implementing advanced technologies in multi-domain operations are carried out by the most economically and militarily developed countries, including the United States of America (USA), the United Kingdom (UK), France, Spain and, even at the organisational level, the North Atlantic Alliance (NATO) or the European Union (EU). They have conducted research on this novel element, generating documents at the conceptual level to reinforce the idea that the achievement of a reliable multi-domain level system is a necessity for future politico-military action. While there are relatively new elements under our analysis, there are some scriptural and already known milestones that literally and theoretically lay out how the concept of multi-domain operations is presented at this time, such as *The U.S. Army in Multi-Domains Operations 2028* (US Army, 2018), *A Strategic Compass for Security and Defence For a European Union that protects its citizens, values and interests and contributes to international peace and security* (European Union External Action, 2022) or *Allied Joint Doctrine* (NATO Standardization Office, 2022). These are milestones of what multi-domain operations mean on the international stage, the basic idea issued at the level of the United States of America being quickly taken up by the allies and, even, by the organisations to which they belong. With regard to artificial intelligence and its applicability in the military sphere, we find a series of views shared by various authors, in particular, *Military Applications of Artificial Intelligence* (Morgan et al., 2020) or at state level by the Ministry of Defence of the United Kingdom through the *Defence Artificial Intelligence Strategy*, which outlines both the importance and the vision of the use of artificial intelligence in the military organisation.

From a methodological point of view, in this study, we will focus on the use of the bibliographical method by analysing and extracting the elements we need, using specialised and relevant documentation in the field of interest. We will also aim to obtain and issue a material based on the quality of the information obtained, given the dimensions imposed by the nature of this study, in relation to the complexity of the problem under investigation.

The future will bring even more novel elements, at a much faster speed than we might be used to, which will be due to the unprecedented development of not only technology but also the human being.

The end of the introduction complements the idea that the future will bring even more novel elements, at a much faster speed than we might be used to, which will be due to the unprecedented development of not only technology but also the human being. In the future, man, by his very nature, will be a fighter who will perpetually try to impose himself in his sphere of interest, so, depending on the size of the space over which his influence extends, even the methods by which he will seek to achieve the status of dominator will differ, the ultimate act being war itself.

DEFINING ELEMENTS OF MULTI-DOMAIN OPERATIONS CONCEPT

In a pluralistic society, such as we find in democratic states today, leading each member of society towards a common vision, specific to a particular ideology, creates constant challenges for the political system and for the structures whose mission is to consolidate societal values. Achieving a secure and stable environment is hampered, firstly, by the hostile intentions of some state and non-state actors and, secondly, by the very diversity of society, with imbalances generated by different ideologies, such as political, ethnic or sexual. Beyond the military aspects of Multi-Domain Operations, the concept has an integrative role in harmonising the military – non-military framework, which gives shape to the whole idea behind the concept. A likely result of the implementation of this concept at national level can be found in the acceptance of the individual as a provider of security and as an integrated part of the military operation process.

Providing an overview of the definition of the MDO concept, in relation to the dimensions required by this paper, will further include a theoretical approach by presenting some defining elements of the connection between this concept and its spheres of influence, in this case military, national and international.

Beyond the military aspects of Multi-Domain Operations, the concept has an integrative role in harmonising the military – non-military framework, which gives shape to the whole idea behind the concept.

Adapting the military architecture to the requirements of the MDO concept is the main point of interest, at the same time taking into account that a multi-domain operational framework is optimal to be able to respond to today’s threats. Even if the basic premises refer to a single whole made up of the harmonisation of military and non-military structures, the scope of action is much more complex because, beyond the capabilities available at national level, the North Atlantic Alliance wants a multinational interaction; moreover, even partner states can be included in this whole with a focus on achieving established objectives. In the same vein, we add the view of the UK Ministry of Defence, which states that conceptual inoculation at defence system level is desired, but with the support of the *“Whole Force”* (Ministry of Defence, Multi-Domain Integration, 2020), further defining the term as the involvement of active military personnel, reservists, civil servants and industry structures to strengthen defence. This aspect reinforces the point made in the first paragraph, namely that the entire society becomes part of the multi-domain whole, making its necessity a reality.

From a military point of view, this concept will be integrated at all levels of military operations (strategic, operational, tactical), being a condition and a desideratum in relation to their interdependence. While the strategic level deals with politico-military aspects, the operational and tactical levels emphasise the military side, where military capabilities are actually deployed to achieve the objectives established on the strategic-operational-tactical pendulum.

At national level, the concept of multi-domain operations and the possibility of its integration depends on non-military variations and the adaptability of the entire defence system, with reference to all its component structures. For a better understanding, we offer the concrete example found in the *Military Strategy of Romania* where *Integrated Joint Force* is defined (MApN, 2021, p. 25) as the concept underlying the way the armed forces operate in an inter-institutional environment in order to achieve established objectives. Starting from the definition of the two concepts, *Integrated Joint Force* and *Multi-Domain Operations*, we can state that from a national point of view, the concept of Multi-Domain Operations aims to include all the elements that have the capability to act together with the armed forces to develop actions necessary to achieve specific objectives or missions.

The approach to Multi-Domain Operations concept by transposing it internationally, taking into account the multitude of factors that can influence the directions of implementation and integration, is a complex one.

The purpose of initiating this concept is relatively easy to understand, aiming to achieve a balance of power between the two poles of power in the international sphere. Using the elements in a practical way to achieve the desired results must be underpinned by an integrative framework between the theoretical aspects and the physical capabilities that can serve this purpose. The problem is imposed by the lack of the necessary infrastructure at international level to demonstrate in real terms what this objective is aiming at. By using the term *international*, we are referring to inter-state cooperation, which first of all requires the implementation of multi-domain notions in national doctrine in order to achieve the inductive meaning that starts from the particular and ends with the general, depending on the defining elements that delimit the terms national and international.

The states that have begun to take a comprehensive analysis of the MDO concept will most likely be the first to succeed in establishing a pluri-domain framework at multinational level for joint action at tactical and operational level, whether in military exercises or in response to a real threat.

The states that have begun to take a comprehensive analysis of the MDO concept will most likely be the first to succeed in establishing a pluri-domain framework at multinational level for joint action at tactical and operational level, whether in military exercises or in response to a real threat.

Aspects relating to the development of capabilities or the integration at doctrinal level of the ideas set out in the MDO concept provide the rhythmicity of its operationalisation process, depending on the capacity of each individual state, the way in which the end state will look like, where the ideal is rendered by integration at military, national and international level.

IMPACT OF EMERGING AND DISRUPTIVE TECHNOLOGIES ON MULTI-DOMAIN OPERATIONS

Through communication and information access channels, specifically the internet, we are given a plethora of details about the latest developments in technology, whether we are referring to robots displaying human traits (United Nations, 2023) or to the capabilities of the cyber domain, where the human resources have been replaced with humanoids, the outcome of the progress of artificial intelligence, capable of presenting news programmes, exclusivity being offered to the public by China (gadget-talk. ro, 2018). Although the non-military environment is leading the technological field, this need for development is also felt in the military sphere, which is why the interconnection between the military and non-military areas must exist, a fact confirmed by the defining notions of multi-domain operations which, in fact, represent a synchronization of military and civilian activities on an inter-domain level (Allied Joint Doctrine, 2022, p. 2).

With the innovations that have emerged in the military field, the practical-applicative side has taken another turn, which requires the doctrinal area to take steps to bring the doctrinal-technical framework into balance.

In recent years, new areas, such as cyber and outer space, have been added to the already established military operations domains (land, air and sea) and their relevance has become increasingly prominent. Over the years, they have been displaying new techniques and equipment aimed at dominating the field and even the battlespace. New technological developments, which have emerged as a quantitative and qualitative response to the information acquired by human beings in the course of history and the revolutionary periods it has witnessed, are increasingly making their mark on the military field as well, with particular emphasis on military science and art. With the innovations that have emerged in the military field, the practical-applicative side has taken another turn, which requires the doctrinal area to take steps to bring the doctrinal-technical framework into balance. The fundamentals of military science will remain the same, here referring to the laws and principles of warfare, which are universally valid, but the way in which the process of operations will relate to them will differ; it is because essential elements such as space and time are *"altered"* in relation to the traditional elements that are already known according to the physical domains. Overcoming these physical limits of the already established domains of operations is a result of these emerging and disruptive entities that can give the possessor an advantage in decision and action.

What Emerging and Disruptive Technologies Are

In order to better understand the subject, the next part of this paper will provide a brief presentation of the technologies in terms of their emerging and disruptive nature, resulting in an introductory part towards their use in the military environment, in relation to the new concepts promoted.

Cambridge Dictionary defines emerging technology as a new technology that completely changes the face of things, or in other words, offers a new perspective on how to approach them. In the non-military environment, the term disruptive technologies is not new, having been mentioned as early as 1995 by Clayton M. Christensen and Joseph L. Bower in an article published in Harvard Business Review.

Cambridge Dictionary defines emerging technology as a new technology that completely changes the face of things, or in other words, offers a new perspective on how to approach them. In the non-military environment, the term disruptive technologies is not new, having been mentioned as early as 1995 by Clayton M. Christensen and Joseph L. Bower in an article published in *Harvard Business Review* (Christensen and Bower, 1995), referring to technology in corporations. Since then, things have evolved and, of course, the notion has found even more industrial applicability to markets and society in general.

At the military organisation level, in addition to the stream of novelty of an applicative-practical nature coming from the civilian area, there is also the notional part, which of course premeditates the emergence of physical elements and which submits this system to a deeper analysis of the doctrinal perspective, having to adopt, in the end, measures to adapt the concept, necessary to maintain the balance between novelty and actuality. Related to the general idea of this paragraph is the syntagm *disruptive military technology* that, as defined by the national security specialist Niculae Iancu (2019), *"is an improved or completely new technology capable of producing* *fundamental changes to traditional security and defence models”*. Disruptive technologies that will find their application in the military, whether at the strategic, operational or tactical level, are artificial intelligence, autonomous weapons systems, quantum technology etc., elements already established at various international congresses, such as the Munich Security Report 2022. The fact that ten years ago we were discussing issues that seemed to be in the realm of the fantastic, which existed only in theory, gives even more freedom to the imagination in the years to come, and just as in the military environment time in units of measurement has become much more compressed, for example in the transmission of information, so it is in the case of technological developments, with the time to materialise the finite products of this infinite field becoming ever shorter.

Probably, a large part of the current emerging technologies, as well as those that will be discovered in the years to come, will find their use in the military field, but, nevertheless, beyond the question of their use and their integration into the military operation process, it is also necessary to mention the economic-financial issue which, in the end, is the driving force behind research in each field and which also contributes to the differentiation between strong and politically-militarily developed states and states that do not have all the necessary resources.

Disruptive Technologies and Multi-Domain Operations Correlation

The initiator of the Multi-Domain Operations concept is the United States of America, which in 2018 published *The US Army in Multi-Domain Operations 2028*, which aims to maintain the advantage and even defeat a potential enemy, almost equally (US Army, 2020, p. 3). The implementation at the national level of this concept is intended to cover the full spectrum caught by the definition of conflict, from peacetime to actual war and back to competition under favourable conditions.

The initiator of the Multi-Domain Operations concept is the United States of America, which in 2018 published The US Army in Multi-Domain Operations 2028, which aims to maintain the advantage and even defeat a potential enemy, almost equally.

In order to start such a process whereby inter-domain action is possible in real time, it is necessary to have capabilities in the sphere of those classified as emerging, because only through a high degree

of technologization can such interconnection be achieved. This aspect of state capabilities and capacities, in the global context, imposes barriers in the implementation of this concept, which is why some state actors are still at an early stage of empirical and even conceptual approach as well as transposition at the level of their own security and defence system.

Achieving this operational framework on a multi-domain and, why not, all-domains level requires time, human and material resources, where we bring advanced technologies to the fore. The characteristics of all these listed elements can lead to the construction of a multi-domain environment where forces can safely perform their missions. With the USA taking a public stand on multi-domain operations, a broad process of capability development has begun, encompassing artificial intelligence, robotics, hypersonic weapons, unmanned drones etc. (The United States Army War College, 2020, p. 21), which is changing the *“face”* of warfare as known to mankind to date.

In this environment, the complexity of warfare is increasing, the way of fighting will be influenced by aspects such as new capabilities that will be developed and introduced into combat to highlight the principle of enemy surprise, the diversity of forces and their mode of action, with contemporary society witnessing the unconventional way of fighting from extremist groups in Afghanistan. Mobility is another feature influenced by technological development, with the war in Ukraine providing a good example of freedom of movement through capabilities deployed and controlled remotely without the physical involvement of human resources on the battlefield.

Mobility is another feature influenced by technological development, with the war in Ukraine providing a good example of freedom of movement through capabilities deployed and controlled remotely without the physical involvement of human resources on the battlefield.

The human evolutionary result of empirically accumulating and acquiring knowledge when referring to the politico-military framework and the conduct of operations is the recognition of the cyber and space domains as operational domains. These two domains cannot function without the existence of emerging technology, or in other words, they can only exist at an a priori level, without giving man a tangible experience. Sustaining and keeping them operational strictly depend on technological development and on obtaining the necessary resources to be able to maintain the necessary technical support.

As known history tells us that human beings are moving towards progress, we will certainly witness new scientific breakthroughs in the future, the scale of which will be transposed both cyber space and outer space.

The role of such technologies is to create a stable interconnection across the five recognised operational domains. In practical terms, they will facilitate communications, the transmission of information in real time, and the connection between the command-and-control elements of the operational and tactical echelons with the forces on the battlefield, in an inter- and intra-domain framework. It is not only time that will become compressed in this multi-domain climate, even space will change in that any action will be known at any location on the globe, and long-range strike capabilities can cover areas of operations with their range, no matter what the battlefield looks like.

The role of such technologies is to create a stable interconnection across the five recognised operational domains. In practical terms, they will facilitate communications, the transmission of information in real time, and the connection between the command-and-control elements of the operational and tactical echelons with the forces on the battlefield, in an inter- and intra-domain framework.

At this level we have an overview and a perspective between the major military players, including the United States of America, the People's Republic of China, the Russian Federation and, at alliance level, the North Atlantic Treaty Organisation, which is promoting a revolutionary competition for supremacy in the economic, political and military spheres. I mention the term perspective because in the years to come, we will most likely have the same major state actors on the international stage, which will be in constant competition to develop their own capabilities.

THE ROLE OF TECHNOLOGY IN ENSURING BATTLEFIELD SUPREMACY

In this chapter we aim to highlight, as the title suggests, how technology, as a general term, can influence the information dimension of warfare and also the implications for decision-making and action. We will also turn to documents issued at the level of the North Atlantic Alliance and by the United States of America, as well as various scholarly works by authors with expertise in the field of study.

In the development of this chapter, we will start by saying that information superiority will lead to decisional supremacy (Perry et al., 2004, p. 3). The first element analysed will be informational superiority, as information is an indispensable element in all fields and it has been demonstrated in many situations, as well as at the societal level, that the holder of information can develop actions with unpredictability. From a military point of view, in order to be at an advantage on the battlefield, it must be possible to obtain real information about the adversary's capabilities, his position in the field or the tactical field, which is why informational battlefield analysis is such an important step in the decision-making process (Wade, 2020, p. 3-3).

The technological progress has definitely influenced the possibility of working with information with the architectural development of C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Research) by the United States of America, specifically at the directive of the Assistant Secretary of Defense who argued that more effort is needed for C4I to provide for the warfighter's needs to accomplish the mission (Architecture Working Group, 1997, pp. 1-2). Thus, this initiative resulted in the first version of C4ISR in 1996, which is an integrative system that, at that time, was aimed at gaining advantage over the adversary, situational and battlefield awareness, and reducing the time between target discovery and taking action. Technological evolution has helped the military system to reach the C4ISR moment, an architecture that has optimised the transmission and use of information for the benefit of its forces.

From a military point of view, in order to be at an advantage on the battlefield, it must be possible to obtain real information about the adversary's capabilities, his position in the field or the tactical field, which is why informational battlefield analysis is such an important step in the decision-making process.

The features of the modern battlefield are constantly changing, its physiognomy is acquiring a new meaning, and new methods are being sought to confront the unpredictability created by the enemy. The aim is to combat the elements that give surprise with the same style of work, a lesson that can be seen to have been learned from past conflicts and wars. As mentioned in the previous chapter, Afghanistan, with the groups that caused instability during the missions carried out by NATO member states on its territory, gave the North Atlantic Alliance, and the United States of America included, the opportunity to learn and to take on board certain lessons. In extenso, we refer to the Taliban insurgency acting against the Western armed forces present on Afghan territory and also to the way in which they used hybrid-type elements and, more often than not, improvised devices to attack certain military structures. These are factors that have led to new conceptual approaches, such as multi-domain operations, in the idea of countering the element of surprise. Of course, in this regard, we have several causes for the desire to implement and operationalise the concept, among which we mention the military and economic development of competing states, namely China and Russia, which have brought to the fore anti-access and area denial systems (Anti-Access Area Denial A2/AD) (Perkins, 2018). The idea that we want to put forward focuses on the creation of compatible systems at the level of all categories of forces and also inter-domain and intra-domain, which can be used to repel threats of any kind, mainly to the security of the Euro-Atlantic area.

The technological derivatives that will be implemented at all three levels of operations – strategic, operational and tactical, in the circumstances offered by the multi-domain complexity, will aim to favour the decision-making process and, ultimately, the operational process by revolutionising the space-time spectrum in all its singularity, in the five established operational domains: land, air, maritime, cyberspace and space.

The technological derivatives that will be implemented at all three levels of operations – strategic, operational and tactical, in the circumstances offered by the multi-domain complexity, will aim to favour the decision-making process and, ultimately, the operational process by revolutionising the space-time spectrum in all its singularity, in the five established operational domains: land, air, maritime, cyberspace and space. *Space and time,* immaterial but brought to the level of resources in the military operational process, require evolutionary approaches to optimise, in practice, what we consider to be quantified by units of measurement. Thus, technology and this multi-domain framework offers the opportunity to unify actions precisely to cover an as large as possible area in an as short as possible period of time, components that will enable command and control elements to make the best decisions and to act accordingly. In this way, the aim is to improve the process of operations in terms of *planning, training, execution* and *evaluation*, in the integrative context of multi-domain operations.

The conduct of military operations has been based on intelligence, in the sense that as long as more details about the adversary and the battlefield are known, forces can be adequately prepared and finally given the opportunity to take the initiative on the battlefield. This element has remained fundamental to the military operation for each of the combatants. The challenge is how the information can be obtained and how quickly it can be analysed and transposed into an operational plan. The collection of data and intelligence is facilitated

at this point precisely by contested domains such as cyber (Ross et al., 2021, p. 23), which create opportunities for cyber attacks whose origin cannot be identified. The vastness of this domain also requires technological development and ultimately digital development to match. As mentioned throughout this paper, technologization is closely linked to economic and financial development, initially being tested in the non-military area, and then elements deemed necessary to the military apparatus become contracted.

Technologization, beyond its benefits, also brings destabilising factors that are difficult to control. In other words, the exposure offered by the digital age in which we find ourselves, also provides an opportunity for non-state actors to make their presence felt in the military sphere, and not necessarily in a positive sense.

However, technologization, beyond its benefits, also brings destabilising factors that are difficult to control. In other words, the exposure offered by the digital age in which we find ourselves, also provides an opportunity for non-state actors (Cyberspace Operations, 2018, p. I-2) to make their presence felt in the military sphere, and not necessarily in a positive sense. The cyber domain is the most exposed to such threats, precisely because it cannot be controlled. After all, it is a domain without limits, or if they are imposed, they cover a small spectrum or rather are meant to provide protection against external threats, which is why malware is also used. These malware attack enablers operate on the basis of abstract elements, which differentiates the cyber domain from other infrastructure-based physical domains, as there are also man-made physical elements within the space domain, such as probes, space stations or various technologies that are in outer space.

Using advanced technologies for cross-domain operations is still a challenge that is generated not only by the competition between state actors with capabilities in this regard, but also by the aforementioned non-state actors, independent or affiliated to organised crime groups that, in return for various benefits, try to cause instability in different environments, especially in the cyber domain, which at the moment is likely to be the most vulnerable.

In the next part of this article, we will analyse how artificial intelligence, as a subdivision of the technological complex, finds its usefulness in the military operation process. This sub-chapter complements the picture that this study seeks to present, that of the use of new technologies in the military environment and, as such, in a multi-domain context. The data provided in this article are intended to generate a deductive perception of the central idea, starting from the correlation between emerging and disruptive technologies and multi-domain operations, continuing with the impact of technology on the information environment and how the transmission of information can be facilitated, and finally looking at how artificial intelligence manages to be integrated into the operation process, as mentioned in the introductory part.

IMPLICATIONS OF ARTIFICIAL INTELLIGENCE IN THE DECISION-MAKING PROCESS

Interstate competition at the political, economic, and military levels among the major global powers is fierce, in particular, bringing to the fore the state of competition between China and the USA, with the former having the capacity to become the strongest rival, according to *The US Army in Multi-Domain Operations 2028* (US Army, 2020, p. 3), in the areas listed at the beginning of the paragraph. China has the capabilities to develop not only in the economic sphere to an even greater extent than it does today, with the *Bloomberg* website ranking it as the world's second largest economy after that of the United States of America (Miller, Curran, 2024), but also in the military sphere where it is making considerable progress. All these aspects are an implicit result of the technological factor, and the two mentioned major state actors are succeeding in revolutionising the technological field with resonance on the military environment too. Thus, emerging technologies such as artificial intelligence have an impact on the way the armed combat will be conducted and the battlefield will look like in the future.

Artificial intelligence is an intensively used concept at societal level, being to a large extent present in everyday life, supporting human actions, but at the same time reflecting a potential threat to human security, for example through possible leaks of sensitive information.

Artificial intelligence is an intensively used concept at societal level, being to a large extent present in everyday life, supporting human actions, but at the same time reflecting a potential threat to human security, for example through possible leaks of sensitive information. However, an improvement of this sector, represented by intelligent capabilities, is under constant development, with each individual state wishing to adapt its infrastructure in such a way as to be able to achieve as many positive results as possible through the use of these technologies. For its part, the military sector, being the main provider of security and safety for the population, is taking steps to implement it at the level of its capabilities in order to achieve speed of reaction in decision-making and increased capacity for action when the situation requires it.

Regarding the use of artificial intelligence in the development of military capabilities, the greatest progress in this regard is being made by the United States of America, but China is also close behind (Kania, Costello, 2018, p. 2). The competition over the development of technologies is, on the one hand, beneficial because it tends to lead humanity to another level of comprehensibility, in a new information age, with the aim of filling in the gaps in the vast *puzzle* of knowledge. However, on the other hand, the same process of technological development may also have repercussions in terms of the escalation of a possible conflict between the major powers, and even if we stop at the cyber sphere, there will still be actions that will have repercussions on the population and the whole security system, because of the volatility of this area.

The competition over the development of technologies is beneficial because it tends to lead humanity to another level of comprehensibility, in a new information age, with the aim of filling in the gaps in the vast puzzle of knowledge.

In terms of decision-making, the use of artificial intelligence is intended to help military leaders make the right decisions by optimising data and processing speed. In practice, the aim is to provide a real-time picture of the battlefield, increasing commanders' knowledge of the situation of troops or their disposition in the field and their material state. The decision precedes the action, which is why we believe that, if a decision is correct and taken in a short time, then the action is likely to have the same effects. Hence, from this we can also extract the usefulness of artificial intelligence in the decision-action correlation, excluding the possibility of its use in the physical field through various technical means that can drive actions to achieve goals without human assistance or through remote guidance.

Artificial intelligence is considered to have the potential to erode the state of stability of the security environment, practically altering inter-state relations, and here we refer to the competitive framework, by bringing to the fore the risk prone to surprise attack (Davis, 2019, p. 14). In the same line of thought, referring to all three levels of the military art – strategic, operational and tactical – it must be identified at which level there are potential risks launched by systems that have artificial intelligence as their operating model. It is relevant to talk about the operational and tactical level and the impact of artificial intelligence on them, but, in fact, a basic framework is created in an axiomatic level, given that the battle is directed within these two levels, and the speed of action is an essential element of the confrontation, hence the need to make timely and correct decisions. On the other hand, given the scale of the strategic level, where we include the political factor, artificial intelligence may not produce the same element of surprise, a point also suggested by James Johnson in his book *AI and the Bomb* (Johnson, 2023, p. 236). The scale and implications of this level as well as the drivers of decision-making are difficult to control under AI. The fact that we can capture, according to the definition of levels, decisions taken in the decision-making process as a result of the effects achieved by actions taken at strategic and operational level reveals a representation of a cause-effect cycle and not of direct implications.

In a multi-domain context, the applicability of artificial intelligence in decision making and action taking is to quickly transmit information, synthesise it and finally provide it to leaders to make the best decisions.

In a multi-domain context, the applicability of artificial intelligence in decision making and action taking is to quickly transmit information, synthesise it and finally provide it to leaders to make the best decisions. The complexity, however, is rendered by the connection it must create at a multi-domain level to meet the needs that fulfilling a mission requires. Interoperability between at least two operational domains is essential according to the concept, and the integration of non-military factors into military operations implies a high degree of use of advanced technologies.

Replacing human resources with artificial intelligence-based equipment changes the physiognomy of the battlespace. In the same vein, we find a statement by former US Secretary of Defense Mark Esper, who emphasised the importance of artificial intelligence for future conflicts because *"whoever holds supremacy over artificial intelligence will control the battlefield for many, many, many years"*. From this assertion we can conclude that artificial intelligence will illustrate a defining element in holding battlefield supremacy in the context rendered by the decision-action ratio.

We consider it important to bring to the reader's attention, at the end of this chapter, some elements consisting of possible risks caused at the decision-making level, both multi-domain and intra-domain, by the use of artificial intelligence. Thus, according to the author Sophie-Charlotte Fischer, in the paper entitled *Armament, Arms Control and Artificial Intelligence*, artificial intelligence systems used in the military are still *"fragile and act unpredictably"* (Fischer, 2022, p. 43), with malware attacks being another weakness of these systems. Such shortcomings can also be found in the use of systems that develop artificial intelligence as well as in the escalation – de-escalation conflict ratio, and the consciousness side of the human resource is brought to the fore, which is guided not only by reasoning but also by the sentimental and spiritual side, something that artificial intelligence has not achieved in its evolution and is still in doubt as to whether it will succeed in the future in obtaining this specific human characteristic. The question is whether or not artificial intelligence systems will be able to reach the emotional barrier in the event of a conflict and allow the necessary time to de-escalate the conflict.

The ethical issues generated by the use of artificial intelligence (AI) are beginning to become increasingly prominent and justified (Coeckelbergh, 2020, p. 5), issues that are captured in Mark Coeckelbergh's book *AI Ethics* where he examines the current and possible future capabilities of using AI capabilities and the limitations they have compared to the human mind and its rational side. With all these limitations that relate to the rational side, AI has managed to achieve a number of results that have surpassed human capabilities, an example being the AlphaGo that managed to beat one of the most titled players worldwide, Lee Sedol[1] (Borowiec, 2016). The aspect that raises questions from an ethical point of view does not refer to the way AlphaGo managed to defeat Lee Sedol, but to the reaction he had to his defeat, which shows emotional involvement as a result of human consciousness and feelings compared to his *"opponent"* that does not emit such human characteristic feelings. The examples given here, which relate to the ethics of using artificial intelligence, are intended to highlight the importance of the way in which new technologies are used and the fact that an evasive approach to issues relating to the typically human emotional side can have negative effects on the *human resource-artificial intelligence* collaborative framework.

AI has managed to achieve a number of results that have surpassed human capabilities, an example being the AlphaGo that managed to beat one of the most titled players worldwide, Lee Sedol.

[1] Lee Sedol, South Korean professional *Go* player.

Artificial intelligence, as an element that marks human existence, must be fully accepted because the future will increasingly expose us as a society to technology and digitalisation, and intelligent systems will be more and more part of human life, regardless of our will because, as we have mentioned throughout the article, man has an evolutionary tendency already demonstrated by the space-time spectrum.

CONCLUSIONS

The implementation of the multi-domain operations concept in all North Atlantic Alliance member states will probably become a necessity and a standard to be achieved by all of them, in all military services, in order to further strengthen the idea of common defence. The national documents of countries that have not taken visible steps in this direction will have to align themselves with Alliance requirements and, at the same time, adapt their internal structures to the conditions that the implementation of this concept imposes on their infrastructure and capabilities. These actions foresee, in particular, the involvement of strategic level command points, consisting of a joint effort with national and international implications on the development of capabilities operating on the basis of advanced technologies, the goal of which may be to generate cross-domain operability.

The doctrinal and strategic mainstreaming of the concept of Multi-Domain Operations provides a unified view of the North Atlantic Alliance and also fosters and facilitates a common vision of how Member States should systematise their working methods to conduct actions in a multinational framework and to create a suitable environment for operationalising the concept.

The doctrinal and strategic mainstreaming of the concept of Multi-Domain Operations provides a unified view of the North Atlantic Alliance and also fosters and facilitates a common vision of how Member States should systematise their working methods to conduct actions in a multinational framework and to create a suitable environment for operationalising the concept.

We believe that the corresponding processes of decision-making and, respectively, the concretization of decisions in action are key elements that emerging and disruptive technologies must augment, by fully or partially supplanting the work of human resources, so that the operationalisation of the concept can acquire an integral form through the maximum use of these resources. Although artificial intelligence is useful in the conduct of military operations and actions, in the context of ISR (intelligence, surveillance, reconnaissance) missions, its potential is certainly much more advanced.

The non-military sphere that foresees applications of artificial intelligence in the functioning rhythm of society, as mentioned throughout this article, faces situations that concern ethics and its derivates when the human resource is replaced. The military system, with the integration and development of military intelligence within its own structures and at various stages of the military operation process, may face difficulties in using these technologies to the extent that they can assume independent decision-making powers in the battlespace. Elementary characteristics of the human being, such as rationality or consciousness, will be elements that may be difficult to attribute to systems based on artificial intelligence, hence the issue of ethics and the main difference at this point between the human factor and this type of emerging technology, concluding that the decision at any level must still be taken by the human being.

The concept of multi-domain operations will be a standard according to which the North Atlantic Alliance and its member states will have to adapt and organise their security and defence systems through the integration and use of advanced technologies.

The future perspective on how to integrate the concept of Multi-Domain Operations at the doctrinal level captures emerging and disruptive technologies as key elements that will underpin the operationalisation process itself, ultimately providing the practicality of this broad concept, which is that, at the architectural level, the battlespace infrastructure will be rendered by the ability to interconnect technological capabilities.

Also, the integration of the two new domains, space and cyber, into the operational sphere is a result of advanced technologies or, in other words, has been imposed by technological development. In the absence of existing capabilities, it would probably be difficult to project a clear picture of cyber warfare, for example, as there is still an anticipatory level based on theoretical segments, an idea that would also be true for multi-domain operations. The concept of multi-domain operations will be a standard according to which the North Atlantic Alliance and its member states will have to adapt and organise their security and defence systems through the integration and use of advanced technologies.

In conclusion, we can add that the generation of an environment in which society will be under the spectrum of security and protection is based on concrete actions that are low risk and where emerging and disruptive technologies can become essential pillars to achieve this goal.

BIBLIOGRAPHY:

1. Architecture Working Group (18 December 1997). *C4ISR Architecture Framework Version 2.0*.
2. Borowiec, S. (15 March 2016). *AlphaGo Seals 4–1 Victory Over Go Grandmaster Lee Sedol, Guardian,* https://www.theguardian.com/technology/2016/mar/15/googles-alphago-seals-4-1-victory-over-grandmaster-lee -sedol, retrieved on 3 February 2024.
3. Chairman of the Joint Chiefs of Staff (8 June 2018). *Cyberspace Operations*, https://irp.fas.org/doddir/dod/jp3_12.pdf, retrieved on 2 February 2023.
4. Coeckelbergh, M. (2020). *AI ETHICS*. London: The MIT Press.
5. Davis, Z.S. (March 2019). *Artificial intelligence on the battlefield*. Center for Global Security Research. Lawrence Livermore National Laboratory.
6. Fedasiuk, R., Melot, J., Murphy, B. (October 2021). *Harnessed Lightning*. Center for Security and Emerging Technology, https://cset.georgetown.edu/wp-content/uploads/CSET-Harnessed-Lightning.pdf, retrieved on 1 February 2024.
7. Iancu, N. (29 July 2019). *Noul dicționar al apărării: tehnologiile disruptive*. Monitorul Apărării și Securității, https://monitorulapararii.ro/noul-dictionar-al-apararii-tehnologiile-disruptive-1-21024, retrieved on 31 January 2024.
8. Johnson, J. (2023). *AI and the Bom – Nuclear Strategy and Risk in the Digital Age.* New York: Oxford University Press.
9. Kania, E.B., Costello, J.K. (12 September 2018). *Quantum hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership*. Center for New American Security, https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-Quantum-Tech_FINAL.pdf?mtime=20180912133406, retrieved on 3 February 2024.
10. Miller, R., Enda, C. (25 January 2024). *US Extends Lead Over China in Race for World's Biggest Economy*. Bloomberg, https://www.bloomberg.com/news/articles/2024-01-25/us-extends-lead-over-china-in-race-for-world-s-biggest-economy?leadSource=uverify%20wall, retrieved on 3 February 2024.
11. Ministerul Apărării Naționale/Ministry of National Defence (2021). *Strategia Militară a României/Military Strategy of Romania*. București.
12. Ministry of Defence (2020). *Multi-Domain Integration*. United Kingdom.
13. NATO (December 2022). *Allied Joint Doctrine*.
14. Perkins, W.A. (2018). *Component Integration Challenges presented by Advanced Layered Defence Systems (A2/AD),* in The Three Swords Magazine.
15. Perry, W., Signori, D., Boon, J. (2004). *Exploring information superiority*. Santa Monica: RAND Corporation.

16. *Prezentatorii de știri TV, înlocuiți cu roboți umanoizi autonomi pe baza de A.I. în China*, https://www.gadget-talk.ro/roboti-umanoizi-autonomi-prezinta-stiri-china/, retrieved on 29 January 2024.
17. Reinhold, T., Schörnig, N. (2022). *Armament, Arms Control and Artificial Intelligence.* Cham: Springer.
18. Ross, R., Pillitteri, V. (December 2021). *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*. National Institute of Standards and Technology – US Department of Commerce.
19. The United States Army War College (2020). *Mission Command of Multi-Domain Operations*.
20. UN News (6 July 2023). *Meet the robots who are making the world a better place*, 6 July 2023. Africa Renewal, https://www.un.org/africarenewal/magazine/july-2023/meet-robots-who-are-making-world-better-place, retrieved on 29 January 2024.
21. US Army (7 July 2020). *Army Futures Command Concept for Maneuver in Multi-Domain Operations 2028*.
22. Wade, N.M. (2020). *The Battle Staff SMARTbook*. The Lightning Press.