STATE-OF-THE-ART TECHNOLOGIES TO BE USED IN COMMAND-AND- CONTROL SYSTEMS

Colonel Dr. Cezar POPA

– Deputy Chief, 2nd Mountain Troops Brigade "Sarmizegetusa", Brașov -

DOI: 10.55535/RMT.2025.3.06

The use of the entire cyber, psychological and informational spectrum is specific to a conflict with variable geometry. The multidimensional operational environment is characterized by the evolution of technology, on the one hand, and by the power of information, on the other hand. It has generated strategies, operational planning processes and appropriate techniques, tactics and procedures. Technological developments have been related to all areas of PMESII. Command-and-control systems based on state-of-the-art technologies are becoming more complex and more efficient. Thanks to the integration and interconnection of new technologies within C2 systems through appropriate architectures, as well as due to the quality of human resources, command-and-control systems have exponentially multiplied capabilities in solving specific situations. Modular organization allows them to adapt, resize and develop in relation to the technological evolution and mutations produced in the physiognomy of military operations.

The architecture of a complex command-and-control system coherently and efficiently integrates sensors, decision-makers, artificial intelligence, performers (human, robotic, highly technological etc.) and support capabilities. All are interconnected (even symbiotically) in subsystems that ensure the effective planning, execution and evaluation of military actions/operations. Achieving and maintaining informational, decision-making and actional superiority throughout the spectrum of military operations, guaranteeing success at strategic, operational and tactical level, is the essential task of command-and-control systems.

Keywords: command and control; artificial intelligence; efficiency; technologies; Information Technologies;

THE IMPACT OF STATE-OF-THE-ART TECHNOLOGIES ON ACTIONS/OPERATIONS IN MULTIDIMENSIONAL CONFRONTATION ENVIRONMENTS

Analysing the impact of *state-of-the-art technologies* implemented in the architectures of command-and-control systems (C2), we consider it important to start from the fact that the current extremely complex and evolved conflict environments are characterized, in addition to technological evolution, by the power of information. Planning to achieve a common goal of the actors participating in the conflict involves exchanging information, similar working methods and joint planning sessions, which, at the strategic level prove to be often difficult. Planning in a multidimensional environment and under the conditions of the specific risks and threats of conflict with variable geometry creates challenges for both civilian and military actors. The military situation and its evolution, together with necessary information, become available in a shorter time and create the possibility of a timely response, absolutely necessary to the often-changing situations in the evolution of a modern conflict. We will briefly present some of the innovations in the field, in order to present the advantages obtained by their implementation at the level of command-and-control systems, having in mind that they have been developed at the tactical and sometimes operational level.

The *Advanced Command and Control System (AC2S)*, developed by the Czech Defence University in 2017, is a concept of how to use modern technologies to increase the efficiency of decision-making (TDDS decision-making tactical support system) and military operations/actions. In addition, the number of military personnel and their equipment for the action/operation to be conducted may also be determined in accordance with the mission requirements.

The concept of *Mosaic Warfare* has a variant of the approach, *Context-Centric C3* (Clark, Patt, Schramm, 2020). This concept assumes that during C2 processes, commanders develop a general approach to an operation that reflects their strategy and the intent of the upper echelon. The commander directs the machine-activated control system through a computer interface, assigns tasks to execute, and introduces estimates for opponents, force size, and desired effect. The machine-activated control system implements Context-Centric C3 by identifying forces (human or robotic/human, technical and weapon) that could perform the tasks

but maintains a manageable control level for the commander. The commander then decides which forces will perform the tasks. It has been driven by the idea that a modular force, capable of composing and recomposing rapidly, could offer several advantages: *Rapid incorporation of new technologies and techniques, tactics and execution procedures, high adaptability of disaggregated forces, high complexity and great difficulty for the opponent regarding the evaluation of distributed and disaggregated forces to determine the intentions and effects desired by the opponent, increased efficiency in the decision-making process, increased area of action, and implementation of an optimal operational strategy.*

Unmanned aerial vehicles (UAVs/air drones) have also experienced rapid military development. Military drones are basically the future of military technology (Eremia, 2020), which is why the list of military drone research and production companies is growing by the day. For example, Iran extensively used Shahed 129 indigenous strike drones in Syria in military operations (2016), Azerbaijan used Israeli UAVs IAI Harop in Nagorno-Karabakh, Iraq used the Chinese CH-4 drone and Turkey's Bayraktar production drones. Turkey has successfully conducted drone operations in northern Syria. The United Arab Emirates used Chinese Wing Loong II drones in Yemen and Libya in 2018. In 2019, Russia used Orion drones in Syria, and France used US drones in Mali, MQ-9 Reaper being the most visible. The Nagorno-Karabakh conflict between Azerbaijan and Armenia (2020) has best highlighted the success of drone operations. In less than 48 hours, Armenia lost 241 tanks, 4 S-300 installations, 2 SCUD installations. Moreover, 39 tanks and 24 BMP were captured. The subsequent proliferation of military air drones in general, and attack drones in particular, has made it possible for the latter to be used more and more frequently in large-scale military operations.

At this moment, we are facing the accelerated proliferation of both state and non-state military aerial drone technologies, which will generate new risks and threats to regional or global security (40 states have acquired and hold military combat or ISR drones, while 28 states are developing UAV technologies). The *"World of Drones"* American statistics place the world's states in three main groups (Ib.): states that have already used combat drones in military operations, states that possess military drones but have not used them (yet) in combat and states that develop technologies for military drones.

Drone units have gained particular importance in the armed forces of state actors. Combat techniques, tactics and procedures have been adapted and folded into the capabilities of drones to provide real-time information. UAVs are used independently or in coordination with attack groups or special forces units

throughout the targeting process – target acquisition/identification, conducting fires and battle damage assessment.

A C5I2SR command-control system (command, control, communications, computers, cooperation, information, interoperability, surveillance, recognition) (Lehaci, 2025, p. 65), in addition to *current capabilities* (Roman, 2017, p. 56) (force command and control, common operating picture and its interpretation, information, surveillance, reconnaissance, operational and tactical planning, air situation and missile defence, joint fire and management of air, naval and land targets, effects management, manoeuvring and synchronization, information operations, force protection, resource coordination, healthcare etc.) need to expand its interoperability, macro-surveillance and recognition at least at regional level if not globally or even in space, in all environments of conflict manifestation.

It is the moment when *artificial intelligence* comes into play, which is increasingly found in the architecture of command-and-control systems. Cyber systems that will emerge from integrated approaches to all conflicting experiences over time will be able to pre-generate in advance combined evolutionary conflict schemes that can be managed before real situations degenerate.

The development of IT technologies has implicitly led to an increase in the number of cyber attacks and increased crime rates. Individuals, corporations and governments have faced extremely varied threats and cyber attacks. For example, in South Africa, crime operation run from the Deep Web segment with the Dark Web section (not accessible to the broad masses) a segment in surface Web, where normal search engines do not have access[1]. In this respect, multifunctional platforms which can fight against cybercrime are needed: the detection and pro-active identification of destructive IT activities, the prevention and reduction of crime through the exchange of information and the protection of relevant users and stakeholders against emerging IT activities in the use of pro-active techniques. However, the context of technological development does not exclude the human element. It remains the most important in the decision-making process supported by an appropriate command-and-control system. Also, through the personnel who serve these technologies with their capabilities, the information becomes available to decision-makers.

[1] Proceedings of the 14th International Conference on Cyber Warfare and Security, Stellenbosch University, South Africa, 28 February-1 March 2019, platform The cybercrime combating Mapimele, Fikile V. and Mangoale, Bokang C., Council for Scientific and Industrial Research Pretoria, 0001, South Africa, e https://scholar.google.ro/scholar?q=Proceedings+of+the+14th+International+Conference+on+Cyber+Warfare+and+Security&hl=ro&as_sdt=0&as_vis=1&oi=scholart, retrieved on 12 August 2025.

Another direction in technology development are the satellites. They can be used separately in all PMESII (Political, Military, Economic, Social, Information, and Infrastructure) domains, but a group of cooperating satellites offers a wide range of advantages. Benefits include optimizing performance in mission execution and reducing or removing errors. Technically and technologically, while there are many benefits for the involvement of a large group of cooperating satellites in the command-and-control process, there are also many challenges. One of the challenges is to determine how cluster/group satellites manage to retain data on other satellites, knowledge necessary for cooperation, to respond promptly and effectively to emergencies/crisis (of any kind) and to optimise the resources needed for their efficient management. The US Air Force Space Vehicle Research Laboratory (AFRL)[2] has researched these challenges and many others by developing prototypes and testing them within AFRL TechSat-21 programme. In command-and-control macro-systems (developed at regional or global level by alliances), these technological components called satellites are extremely necessary because of their highly developed location and communication capabilities of any kind. Moreover, they can be even equipped with defensive or offensive combat and/or combat support systems, when space is found among the conflict environments. The command-and-control approach using satellites provides the ability to integrate traditional approaches with artificial intelligence (AI) and non-AI. Problems related to the integration (knowledge and cooperation) of many components can be solved by applying solving techniques for subcomponents (intelligent agents) and integrating individual solutions to reach a final, complete solution.

With regard to the concept of space warfare (ground-space operations – *ground attack of satellites*, space-space operations – *satellites attack satellites*, space-ground operations – *attack executed by satellites on ground* and combined devices), our opinion is that, considering it a *symbiosis of architectures* of the ground-based and satellite control systems, in conjunction with the control part of the execution of military or non-military operations by disaggregated forces, the concept of *mosaic warfare* may be the optimal solution for models of command-and-control systems extended at strategic level, with the possibility of rapid adaptation to the changing geometry of latest conflicts.

Any nation with space intelligence gathering capabilities has also the possibility of optimal use of its high-performance ground attack installations (high-precision

[2] *"TechSat 21: Advanced Research and Technology Enabling Distributed Satellite Systems"*, Overview Briefing of TechSat 21, http://www.vs.afrl.af.mil/vsd/techsat21, retrieved on 18 August 2025.

striking systems) and vice versa. Thus, the best-performing missiles become somewhat useless without observation and information from space.

Specifically, the results obtained in identifying the *impact of state-of-the-art technologies and artificial intelligence* on operations conducted in the *multidimensional conflict environment* will be presented through a brief SWOT analysis.

A. STRENGTHS	B. WEAKNESSES
Developing the efficiency of decision-making process: - rapid (real-time) transfer of information; - rapid, comprehensive, synthetic, analytical and objective analysis of specific situations in the field/area/region; - automatic generation of COAs based on big-data access and analysis algorithms used by artificial intelligence embedded within C2; - quick force taskorg set up, in accordance with the mission requirements (number of military and equipment) necessary to carry out the action/operation; - optimising/updating the organisation of military systems as well as doctrines, primarily by changing the ratio of human resources and materials/equipment involved; - The concentration of human resources will be on the really relevant/important/critical aspects; **Development of response force capabilities:** - Leads to increased speed of military operations: 1. The huge amount of data available may increase the speed of decision-making, but if the decision-making process is overwhelmed with data/information, it may decrease the speed of this process in the absence of adequate management tools.	- Partial replacement of the human factor in the decision-making process/how far certain tasks should be delegated to the AI (e.g. during the Cuban missile crisis, human decision-makers changed their minds about actions/attacks. AI would not have done so in the absence of actual data to generate this change); - Possibility of decreasing or losing human control in the execution of missions using robotic weapon systems; - The need for exponential growth of measures to protect information and artificial intelligence systems; - COAs generated by artificial intelligence lose sight of military art elements, data and information analysis being algorithmic, and may be overlooked essential human-specific analytical variables; - Involves the error-free use and/or integration of automated platforms – robots, drones etc.; - Creates problems related to moral/ethical aspects as well as those concerning the legality of the use and actions of Artificial Intelligence; (not yet really debated/ profound discussions on moral issues; morality and legality are determined by the power brokers/those who make the laws/ leaders);

2. Increases process's speed and boosts decision-making process; 3. Increases the quantity and quality of processed information and products/ processes, as well as the efficiency of processes /activities; 4. Significantly/decisively contributes to increasing the level of understanding of the data provided by the multitude of sensors. - disaggregated force (capable of composing and recomposing rapidly adapted to the specifics of the mission); - reducing human losses by using advanced (robotic, automated) combat technologies; - ergonomics in the use of forces and equipment by performing large-scale operations or surgical blows, as needed. **Communications:** - communications and portable technologies that communicate within networks at soldier level; - different networks communicate with each other, - facilitating the creation of tactical, operational, strategic information networks; **Issues relevant to Command Points within C2:** *CP mobility* is increased by using modular (container) infrastructure and mobile networks are built up based on miniaturiarisation of components and terminals, for use in heavy humidity conditions etc. *Secure wireless.* Currently, secure IP-based transmissions can only be made from static locations, but state-of-the-art technology will allow mobility.	- Developing AI is a task in itself; - AI is a real challenge – training an AI is done through real processes and activities, not simulated, such as training in a military range. E.g.: in 2003 a Patriot system operating on automatic operating mode shot down a RAF (UK) aircraft, and a few months later, in another similar incident, a USAF aircraft was shot down; **Communications:** It is necessary to secure portable devices for use in military networks (military personnel do not have individual secure tactical terminals); increase in the need for IT specialists; processing speed and storage capacity are critical as the amount of data increases exponentially and the human factor cannot process them;

Cyber Security – physical destruction can be caused by IT means (e.g. Stuxnet – destruction of Iranian centrifuges); use of troll factories in shaping public/ social agendas and opinions at the level of a society (e.g. fakenews phenomenon, Russian troll factories). *IT/network access* – building the common operating picture, access and processing of signals and images/maps, ISR integration systems, security etc.; (one possibility is to access information stored in cloud – see US government contracts with IT giants for cloud capabilities). Low-altitude satellite networks and other civilian infrastructures can be used for military action by encrypting signals and data, as they make it impossible to completely destroy the system/multiple redundancy (similar to the STAR system).	
B. OPPORTUNITIES **On the efficiency of the decision-making process:** - instant access to specially designated or international databases, information; - extremely fast processing of data and information (with an immeasurably higher speed than the possibilities of the human brain); - the connection and interconnection of command-and-control systems in extensive multinational operations; - the use of C2 modules in a rubic or mosaic mode (as a whole or in combination, according to the specifics of the operation and at the required level); - architectural flexibility of the platforms used and C2 modules;	**D. THREATS** - the real factor of the databases used, - neutralising C2 systems or intelligent weapons systems through imminent cyber attacks; - the great influence of artificial intelligence on human decision-making (decision based on experience, knowledge and talent can be overlooked); - taking control of weapon systems by artificial intelligence or the enemy through cyber attacks on the infrastructure of poorly protected C2 systems; **On communications:** - Connectivity and traffic levels raise access/ risk/vulnerabilities issues;

- simultaneous action with the response cells actions planning; - can contribute to the construction/ validation/verification of a context, a reality, in the military field of the Common Operating Picture/Situation Awareness. - immense power in identifying and classifying various objects/equipment/ threats/individuals, with an incomparable precision and speed higher than man. - Building relevant databases can facilitate the success of military operations 1. Example: based on databases with images of enemy equipment, a vector can prioritize its first attacks, in which impact zone can cause the most damage, make difference between friend or foe etc.; 2. Large enough biometric databases allow for the construction of diagrams/networks and the extremely rapid identification of critical elements/objectives in a human network – see Baghdad in the Gulf War, Afghanistan, criminal databases... 3. Increased accuracy leads to a decrease in the likelihood of a misperception/mistake and an escalation of the security situation can thus be avoided. **On the disaggregated, technological and robotic force:** - Rapid implementation of new technologies and techniques, tactics and execution procedures; - High adaptability of disaggregated forces; - Complexity and great difficulty for the opponent regarding the evaluation of distributed and disaggregated forces to determine the true intentions and opponent's desired effects;	- The Internet of Things will generate huge amounts of data and metadata, and its control and access may be restricted or may generate disputes. E.g.: Some companies may be restricted from entering the market; - Access to metadata can provide relevant data and if pieced together can lead to critical information. E.g.: Cambridge Analytica scandal – Brexit, US election; - Modelling/influence the public opinion/a critical mass to have a desired reaction (action or passivity). E.g.: elections won at thresholds below 5%, by presenting a small number of voters/electoral passivity. E.g.: Sun Tzu – *"win a war without waging it"*.

-Increased efficiency in decision-making process during the execution of the mission; - Increase in the area of operations by ergonomic use of force; - Optimal operational strategies – exponential reduction of resource losses of any kind; - By increasing the degree of automation, more robotic equipment will be integrated at the tactical level, while the human resource will be more engaged in the analysis and decision-making process.	

TECH INTEGRATION WITHIN THE MODULAR AND FLEXIBLE COMMAND-AND-CONTROL SYSTEMS

Integrated systemic approaches into the art of operational planning capture the fact that up-to-date technologies ensure information flows at all levels (strategic, operational and tactical).

The starting point for optimizing conflict with variable geometry command- and-control systems is that they *must extend* their interoperability, macro-surveillance and recognition capabilities.

The equipment used is based on the latest technological discoveries and developments. For example, Network Enabled Ability (NEC), a term used at NATO level for the system designed to achieve greater military effect through integrated use of information systems, integrates all the equipment and technology. Artificial intelligence is increasingly integrated into highly complex IT systems that are able to learn for themselves from situations that are managed with their help. Researches in this field have developed artificial intelligences to work on the same principle as the human brain. They can analyse algorithmically and synthetically, and can generate quick solutions that are absolutely necessary in time sensitive situations in the decision-making process. The commander may be offered, in a relatively short time, already analysed COAs, using variables that were previously fed to the system, and using a comprehensive database. The decision will be made much faster, whether a system-generated course of action or an intuitive or a combined course of action is taken. However, the human factor plays the most important role.

The *integration and interconnection of subsystems and technologies* necessary for the operation of command and control is important in the decision-making process. Identifying and/or constructing tools to analyse the operational environment and to identify the procedures for action necessary for command-control, under the conditions of managing conflict-specific situations with variable geometry becomes imperative.

The *process of making forward-looking and correct decisions* in these situations is conditional on adapting military action to real strategic situations and addressing all areas of conflict with variable geometry in planning and leadership. In this respect, the modularity of the command-and-control systems will lead to increased structural and actional mobility. The use of high-performance technologies will lead to a significant increase in decision-making and action capacity on: increasing the distance of action and precision that will make it possible to selectively and punctually engage objectives; the ability to choose the target effect from a wide range of non-lethal and lethal effects, which will give the military decision greater flexibility; achieving the state of confusion necessary to obtain surprise and victory through processes of psychological, information warfare and misleading operations; increase responsiveness, optimizing management and achieving the viability of technical systems.

The result of the use of high-performance technologies, their *integration and interconnection of the subsystems at C2 level* will result in: significant increases in the mobility of systems and subsystems and decision-making capacity; increasing the potential of forward-looking; broadening the range of planned and conducted operations; diversification of decision-making and management procedures and management of military or non-military actions/operations; solutions for multidimensional protection of forces/objectives.

THE ROLE OF INFORMATION TECHNOLOGIES AND ARTIFICIAL INTELLIGENCE IN OPTIMISING DECISION PROCESS

Information technologies developed to date in the military ensure information flows within the forces command and control, obtaining the Common Operating Picture and its interpretation, in the field of intelligence, surveillance, reconnaissance, strategic, operational and tactical planning, air situation and missile defence, joint fires and management of air, naval and land targets, effect management, manoeuvring and synchronization, information operations, force protection, coordination of resources, healthcare etc.

In the face of the risks and threats of a conflict with variable geometry (Mituleț u, 2019), real-time communication between national or multinational forces, command and support structures, as well as between strategic leadership elements or other elements with security and defence responsibilities is a determining condition in achieving the desired effects throughout the execution of non-military or military operations. Information and communication technology have the lead position, both in terms of the number of innovations and their impact in the military field. At the command-and-control level, regardless of the structure, field or level at which it is conducted, cognitive systems will construct *scenarios based on relevant assumptions and contextual data,* offering decision-makers alternatives/COAs or, in certain situations, making their own decisions with direct impact on operations. This effect of the sharing data and information by computers and people is of most importance in the decision-making process. The next level is to *model data and information* and classify them semantically to *reconstruct virtual possible scenarios from reality.* It is the level to which all command-and-control systems used in the effective management of latest crises and conflicts tend, particularly of those whose geometry is constantly changing.

Information technology is defining, but the human element gives it the shape we perceive. Digital development and new information technologies have led to significant changes in the preparation and use of the human resource involved in both decision-making (architecture, structures and infrastructure) and execution (technical and equipment, combat and armaments). The global military trend is to transform C2 architectures and models folded into the current requirements generated by the variable geometry conflict using the effects generated by new information technologies based on digital evolution. Artificial intelligence implemented in command-and-control systems will anticipate human intentions and provide options/variants/scenarios/COAs before we actually need them.

In the military field, information is managed by intelligence structures/units (Intelligence-INTEL). The role of INTEL units is to provide decision-makers with a complete picture of actors participating in the conflict and the conflict environment (or the operational environment – in a narrower understanding of the conflict environment). This image should include the actors' status (temporary objectives, strategy, doctrine, tactics, composition, capabilities, gravity centres, vulnerabilities, capabilities and intentions). INTEL must provide a complete picture on the enemy, its culture, traditions and history, shaping its societal and ethnic environment. An information process carried out in support of the decision-making process must be timely, sound and accurate. It is based on the need for the rapid information

flow from all sources available through state-of-the-art information technologies. The information shall be collected on the basis of the Commander Critical Information Requirement (CCIR) after it has been previously identified.

An information cycle comprises four stages – planning, collection, processing and dissemination of the final product, and information technologies are undoubtedly the component that ensures the accuracy and speed of the process and implicitly of the information cycle. The information thus processed ensures the Comprehensive Picture of the Operational Environment (CPOE) in terms of the development of the main characteristics of the operational environment (terrestrial, maritime and air) as well as of the political, military, economic, social, infrastructure and information fields of opponents, allies and neutral actors that may influence operations of any kind.

The complex and continuous process of planning, coordination, synchronization and conducting information activities in order to achieve the desired effects on the ability of understanding and perception, the will and capabilities of the opponent or other entities, in support of the achievement of military objectives, while at the same time ensuring the protection of their own is also supported and is based on state-of-the-art and ever-improving information technologies. This process consists of performing information operations (Info Ops).

Advanced information technologies are used in shaping operations, focused on changing or strengthening the perceptions and attitudes of the opponent or potential opponent, or in information protection activities, focused on maintaining freedom of manoeuvre in the information space by defending the data and information that support the decision-making process. There are also attacks on data and information systems that support the opponent or potential opponent and on those information systems, surveillance and target acquisition systems (Intelligence, Surveillance, Target Acquisition and Reconnaissance/ISTAR) that use information to support the decision-making process.

Information technology generates developed capabilities, tools and techniques or key elements specialized in information activities. For example, information technology helps PSYOPS (different from public information) to have direct control over the content, dissemination and audience to achieve objectives of supporting the general interests of force, weakening the combative will of opponents or potential hostile target audiences, strengthening the beliefs of friendly or allied target audiences, attracting support and cooperation of neutral and undecided, supporting reconciliation and tolerance actions, promoting a positive

image of military forces deployed in the theatre of operations and countering hostile psychological actions.

Operation security requires identifying and protecting critical information considered Essential Elements of Friendly Information (EEFI) and can only be achieved through state-of-the-art information technology. Information security ensures the confidentiality, integrity and accessibility of information through procedural, technical and administrative control based on unbeatable information technology.

Misleading the opponent is achieved by manipulating, distorting and falsifying information and applying both informational and traditional means and techniques and technologies.

Electronic Warfare (EW) supports Info Ops by using advanced technologies so that critical information underlying the opponent's decisions and the systems that carry this information is affected. Commanders can use EW activities in the context of influence measures, and prevent the opponent from exploiting these opportunities.

Information technology also supports the engagement of key leaders by facilitating bilateral discussions between commanders and their military and civilian correspondents at the same level of influence, speaking on various occasions, in the presence of the media and/or key decision-makers, in the preparation and dissemination of interviews, for a particular media segment, with broad coverage and a great influence on the targeted objectives, conferences prepared to address specific topics of interest, with potential for influence.

The opportunity and efficiency of computer network operations (CNO) depend on the degree of dependence of the opponent on the information technology used. It materializes through executed attacks on the opponent's computer networks and the defence of their own networks. Attacks are carried out by feeding flawed codes (computer viruses) and manipulating data for the purpose of modifying the characteristics and performance of devices or of disclosing the information contained therein by exploiting them. Maintaining the capabilities that support the decision-making process is essential for the execution of operations. A procedure is therefore being developed for maintaining a defensive attitude and using protective techniques to monitor and penetrate information systems also on the basis of existing and permanently developed information technologies. The aim is to identify and define the type of attack and to have an appropriate response through actions to limit/delay and/or wind up their effects.

The challenges of artificial intelligence in the field of security and defence are not few and must be taken into account for current conflicts with variable geometry or for future ones. On this date we are witnessing a major advance in the use of AI in all areas of life, this type of technology providing a more comfortable life for those who use it. But AI has also a strong negative social impact by reducing personal privacy and can lead to a climate of insecurity if not properly managed. Moreover, AI has the ability to self-learn. It contributes to the *redefinition of both the security and defence concept, and strategy and the operational planning process* where planning for a potential conflict campaign/operation is required. In this respect, the command and control structures at the strategic, operational and tactical level need to develop capabilities to anticipate potential attacks on national or regional security (in the context of a regional, multinational, extended conflict) and on the security of forces in the area of operations (for operational-tactical level).

AI can have beneficial effects (efficiency of decision, protection of force, reduction in the number of human victims etc.) but also destructive ones (in the field of security, the future of humanity) (Ene, 2019). This technology poses a major challenge for command-and-control systems and beyond. It is absolutely necessary in the conditions and situations created during conflicts with variable geometry for timely management through analysis and informational synthesis of the rapid change in the geometry of conducted operations or even of conflict in general. At the moment, we consider that it is irreplaceable in the architecture supporting national, regional, global or even space defence and security. The fight goes for supremacy in the field of information technology and artificial intelligence in order to have global control. However, the implementation of AI in *command-and-control systems* and *weapon systems* without clearly drawing its limitations in decision and control and without maintaining absolute control by the human factor over it can have a destructive effect. The questions that need a quick answer are those related to how far should certain tasks be delegated to AI. For example, during the Cuban missile crisis, human decision-makers changed their minds about actions/attacks. AI would not have done that in the absence of real data to generate that change. Another question that arises is about moral/ethical issues as well as concerning the legality of the use and actions of artificial intelligence (Development of AI is a task in itself and has not yet been actually debated/deep discussions on moral issues). A weapon system using artificial intelligence is initially programmed (target determination and destruction) and later it will schedule itself on the basis of AI. How will we control these completely independent weapons? When and if an autonomous system kills, who is responsible for that action? (forbes.com, 2019).

We all know that a soldier's mission is particularly dangerous, but certain missions that soldiers must carry out are extremely difficult, if we are talking about clearing a building where enemies are found or deactivating a bomb. What if we had the ability to send robots to carry out such missions instead of humans? If something did not go according to plan, we would just lose material resources. We see important benefits of this technology, but can we be sure that this approach will not completely change our way of life? A real challenge is to train an AI through real processes and activities, not simulated, such as training soldiers in a range. For example, in 2003 a Patriot system operating on automatic operating mode shot down a RAF (UK) aircraft, and a few months later, in another similar incident, a USAF aircraft was shot down. The US successfully uses unmanned aircraft that carry out surveillance missions and can launch missiles at targets (science.howstuffworks.com). The effectiveness is undeniable but there is controversy over the morality of these actions. While the drones are doing their job at a height, the enemy has absolutely no chance of defence (The Nagorno-Karabakh conflict of September 2020 – Armenian losses: destroyed 241 tanks, 4xS-300, 2xSCUD and captured 39 tanks and 24 BMP all within 48 hours since the outbreak of the conflict and all as a result of drone action. Azeri losses – unspecified). In this scenario, a human operator will decide when that drone will open fire. The use of weapon systems or autonomous weapons requires a thorough risk analysis, as technology can quickly replace the human factor due to information processing speed and algorithmic decision-making speed.

In conclusion, command and control should not be delegated from the human factor to AI. It is necessary for the human factor to have control over AI and command-control over disaggregated forces with rapid aggregation capability, fully or partially robotic.

CONCLUSIONS

The evolution of artificial intelligence and information technology in recent years is significant and unavoidable. Today, we are no longer talking about computers that are capable of generating solutions, following pre-defined algorithms, but we are talking about computers and devices that have the ability to develop their own learning capacity. With reference to the security and defence subjects and applicability in the military field, we consider that new information technologies in conjunction with AI will develop the *decision-making process* specific to operational planning developed using complex and modular command-and-control systems at all hierarchical levels. AI terminals will be found in all automated, robotic weapon

systems within the disaggregated forces (with the possibility of rapid aggregation on the specifics of the mission to be executed) reducing the risk of human losses, increasing the level of force protection, increasing reaction speed and firepower etc. Artificial intelligence has a potential role to play in reducing the use of human resources in various fields, processes or activities, but it requires the use and/or integration of digital, automated platforms as well as robots, drones etc.

In the sphere of communications, technology is evolving rapidly, the trend being to have communications and portable technologies that communicate within networks from the military structure level to the individual level. It is preferable to have the possibility that different networks (belonging to or serving different structures) to be able to communicate with each other (tactical, operational, strategic). This level of connectivity and traffic (e.g. 5G) can, however, raise access issues, create risks and generate vulnerabilities. Building the Common Operating Picture requires access and processing of signals and images/maps, ISR integration systems, security etc. AI can have quick access to information stored in cloud (see US government contracts with IT giants for cloud capabilities). For the human factor, the processing speed and storage capacity *are critical* as the amount of data increases exponentially and the human factor cannot process and store them. From this point of view, it is recommended to implement AI at the level of processing data stored in macro-exponentially growing databases.

Low-altitude satellite networks and other civilian infrastructures can be used for military action by encrypting signals and data, as they make it impossible to completely destroy the system with multiple redundancy (similar to our STAR system).

Therefore, *the impact of the state-of-the-art technologies* implemented in C2 systems is manifested concretely *in terms of data traffic, accurate analysis of information and its dissemination, efficiency of decision-making and optimising*[3] *and achievement of common objectives for actors participating in the conflict*[4].

BIBLIOGRAPHY:

1. Clark, B., Patt, D., Schramm, H. (2020). *Mosaic warfare exploiting artificial intelligence and autonomous system to implement decision – center operations*, Center for Strategic and Budgetary Assessments, https://csbaonline.org/research/publications/mosaic-warfare-exploiting-artificial-intelligence-and-autonomous-systems-to-implement-decision-centric-operations, retrieved on 10 August 2025.

[3] By implementing AI in information systems and facilitating AI access to big data databases, thus generating algorithmically-based comparative analyses, rapid and with results that materialize in generating concrete and coherent courses of action as well as in establishing taskorgs by type of mission.

[4] Through rapid exchange of information, similar working methods and availability for joint planning sessions.

2. Ene, P.-V. (2019). *Beneficii și riscuri în domeniul inteligenței artificiale*, *Conferința științifică internațională Gândirea militară românească*, București.
3. Eremia, C. (2020). *Epoca războaielor dronelor aeriene s-a instalat definitiv?,* https://monitorulapararii.ro/epoca-razboaielor-dronelor-aeriene-s-a-instalat-definitiv-1-31794, retrieved on 22 August 2025.
4. Hariuc, N. (2019). *Spațiul, un nou câmp de luptă,* https://www.rumaniamilitary.ro/spatiul-un-nou-camp-de-lupta, retrieved on 17 August 2025.
5. Lawrence, F. (2019). *Viitorul războiului, o istorie,* translated by Corina Hădăreanu. București: Editura Litera.
6. Lehaci, N.-T. (2015). *Tendințe în evoluția sistemului de comandă și control la nivel operativ*. București: Editura Universității Naționale de Apărare "Carol I".
7. Mitulețu, I. (2019). *Siria – spațiul unui conflict cu geometrie variabilă și consecințe imprevizibile,* in *Revista Academiei de Științe ale Securității Naționale*, no. 1.
8. Proceedings of the 14th International Conference on Cyber Warfare and Security, Stellenbosch University, South Africa, 28 February-1 March 2019, platform The cybercrime combating Mapimele, Fikile V. and Mangoale, Bokang C. Council for Scientific and Industrial Research Pretoria, 0001, South Africa, https://scholar.google.ro/scholar?q=Proceedings+of+the+14th+International+Conference+on+Cyber+Warfare+and+Security&hl=ro&as_sdt=0&as_vis=1&oi=scholart, retrieved on 12 August 2025.
9. Roja, Al. (2018). *Transformarea digitală – provocare, risc sau oportunitate?, Research and Education,* no. 2, www.researchandeducation.ro, retrieved on 22 August 2025.
10. Roman, D. (2017). *Abordări sistemice integrate în arta planificării operaționale*. București: Editura Universității Naționale de Apărare "Carol I".
11. *"TechSat 21: Advanced Research and Technology Enabling Distributed Satellite Systems"*, Overview Briefing of TechSat 21, http://www.vs.afrl.af.mil/vsd/techsat21, retrieved on 18 August 2025.
12. http://economie.hotnews.ro/stiri-it-12494265-kaspersky-exista-dovezi-solide-sunt-legaturi-stranse-intre-armele-cibernetice-stuxnet-flame.htm, retrieved on 13 August 2025.
13. https://science.howstuffworks.com/robots-replacing-soldiers1.htm, retrieved on 22 August 2025.
14. http://windows.microsoft.com/ro-ro/windows/viruses-faq#1TC=windows-7, retrieved on 22 August 2025.
15. https://www. darpa.mil/news-events/, retrieved on 12 August 2025.
16. https://www.dw.com/ro/irakul-ringul-de-lupt%C4%83-americano-iranian/a-51853825, retrieved on 13 August 2025.
17. https://www.forbes.com/sites/cognitiveworld/2019/01/14/the-weaponization-of-artificial-intelligence/#4877c372368 6, retrieved on 22 August 2025.
18. http://www.vs.afrl.af.mil/vsd/techsat21, retrieved on 22 August 2025.