Bulletin of ”Carol I” National Defence University
10.12753/2284-9378-20-23

THE INFORMATION DIMENSION OF THE MODERN BATTLEFIELD

Maj. Advanced Instructor Petre-Răzvan ENACHE, PhD*

The current security environment is characterized by complexity and dynamism, being influenced by multiple challenges. The proliferation and diversification of information systems in the context of the technological revolution result in different effects among which the emergence of different actors that are present in the areas of military operations, especially given the more and more complex types of threats to the contemporary security environment. The new technologies brought by the information revolution become the main means able to determine the increase of the efficiency of military actions and the achievement of the surprise in the battle space. A major concern of military structures in terms of operations, regardless their level, is achieving the information advantage / upper hand creating the creating the conditions necessary for attaining success on the battlefield, avoiding as much as possible, losses of any kind. The new approach of the information-related activity, developed through appropriate actions, is able to ensure the correct asymmetric advantage in the context of any challenge.

Keywords: information environment; information systems; intelligence; information advantage; security.

”Know thine enemy, and know thyself; in a hundred battles you will not expose yourself to any danger”[1], said the great Chinese strategist Sun-Tzu, in his well-known work, *The Art of War*.

I set out to begin the article with this quote to emphasize the need to decipher and understand the information dimension of the modern battlefield or, rather, of the battle space so that we can ensure those advantages that can guarantee our success with as little loss as possible. Achieving the ultimate goal or, in other words, fulfilling the mission depends, to a large extent, on obtaining and maintaining the information advantage, essential during the planning and conduct of military operations in the context of the contemporary security environment. I believe that it is essential to understand – at all times – the nature of the threats that are becoming increasingly complex and diverse, which means that information is essential in understanding the environment in which we operate.

Defining aspects of the contemporary security environment

The current security environment is characterized by complexity and dynamism, being influenced by multiple challenges. This is mainly due to changes in the military strategies of some states due to the emergence of new types of threats different from the classic ones specific to conventional warfare.

Romania, as a member state of the North Atlantic Treaty Organization/NATO and the European Union/EU, has undergone a process of reviewing its defence strategy in recent decades, identifying optimal solutions to protect national interests against current risks and threats. At the same time, a priority of our country is represented by the fulfillment of the commitments in terms of security and defence assumed within NATO and the EU for consolidating the position of security guarantor in the eastern flank of NATO, especially in front of new types of increasingly complex and diversified threats.

We are witnessing, in the last decades, a real technological explosion with complex and extremely fast changes and evolutions of the technological discoveries in which innovation has its say. What is today of the latest generation becomes obsolete in a very short time because other more efficient systems appear and are subject to research so as to be permanently updated to the requirements of the times. In fact, I could say that the updates are more the result of market requirements as users do not have enough time to implement and get used to this technology because a much more current and efficient one appears. It is a very useful aspect because the technology comes in support of the effort made and leads, in this way, to very good

***”Carol I” National Defence University**
e-mail: *razvann_enache@yahoo.com*

results and with as few and insignificant errors as possible. It is inevitable that these developments will have effects in the information field, their evolution being, I consider, directly proportional to the results and effects obtained by those operating in this increasingly complex field, namely the information field.

Recent studies and experiences have shown that, periodically, with a very high frequency, military communications and information systems need to be modernized, due to the fact that the pace of development of information and communications technology is exponential compared to other areas of activity and is due to a great measure of the diversification of the beneficiaries’ requirements. Also, an important role in the need to modernize the systems is played by planned and unplanned moral wear and tear.

In recent years, the dimensions of military conflicts have changed radically due to their asymmetrical nature and speed. The implementation of modern technologies within the Romanian armed forces allowed a ”compression” of space and time in the tactical field, which led to the imposition of a faster pace of execution of military actions in the areas of operations.

In the current military conflicts, the information is what dictates the conduct of future operations. No conflict is triggered until after the execution of large-scale intelligence actions by specially trained forces in this regard. Also, the paralysis of the communication system is a desideratum that the enemy will try to reach both before the outbreak of hostilities and during the execution of operations.

It is very clear that these technological developments lead to changes in the conception of modern armies in terms of the organization and equipment, training and use of different military structures in operation, as well as the protection and approach of different types of conflicts. In this regard, it is important to analyze the characteristics of information media, especially the military one in the context of the global information environment.

Military information environment

Studying and analyzing the main provisions in the field, as well as the literature, I consider the global information environment as consisting of personalities, organizations, systems, etc., most of them not under military control or central governing bodies that carry out collection activities, analysis, processing and dissemination of information of any kind to the general public.

It is clear that all military operations take place within the global information environment which has positive or negative effects in all areas of activity. It is not infrequently that we have noticed that some aspects specific to military operations are brought to the attention of the general public in almost real time and this is due to technological evolution. The speed with which they are transmitted, most of the time, being aspects with a negative touch or that affect the image of the military organization, does not offer the possibility to be filtered even if they are partially or totally untrue. All this determines a certain behavior in the conduct of military activities in any situation in order not to give the possibility to exploit a certain detail and to give a different meaning than the real one to the existing situation.

Part of the global information environment, we discuss about the military information environment in which we find ”information systems and organizational structures of their own and of the adversary, military and other categories that support or significantly influence military operations. It must provide at least the following facilities: connection of home terminals to systems in the area of operations, transition from peace to war within the planned timeframe or even sooner, provision of technical support for real-time communications necessary for the fulfillment of missions and cooperation between all categories of military, economic, social structures, as well as local, zonal and national political-administrative ones. Within this environment, military leaders will lead the operation (fight) and will face many new challenges and various situations”[2].

The multiplication and diversification of information systems in the context of the technological revolution implies multiple effects, including the emergence of a diversity of actors present in the areas of military action, especially given the emergence of new and more complex types of threats to the security contemporary environment. This certainly influences the way military operations are planned and conducted.

In this regard, we identify part of the information infrastructure of ”defence resources required for the transfer and processing of information, data storage and display, technical means for command

and control, research and other categories of means for transmitting voice, still and moving images, multimedia services etc. useful to the defence system”[3].

The wide spatial development and the unprecedented diversification of the technical means used for collecting, transmitting, storing, processing and distributing (disseminating) intelligence have made the role and importance of information systems continuously increase in all fields of activity. In the military, it has become the main means for acquiring and maintaining the information superiority, increasing the command and control capacity (management), as well as for ensuring the possibilities of time and space synchronization of the activities carried out.

The new technologies of the information revolution become the main means, able to determine the increase of the efficiency of the military actions and the achievement of surprise in the combat space.

In the conditions of the creation of the information and knowledge society, in which information and knowledge are paramount for the organization and execution of human activities, the information systems become even more important than the resulting products or services offered by the organization. Therefore, the concentration of human activities within each organization will be performed so as to obtain and process information, accumulate knowledge and use it at a higher level of human and artificial intelligence, which will lead to the proliferation of modern equipment and symbolic products (software, databases, etc.) simultaneously with the relative decrease of physical products. As a result, it will tend to dematerialize and disintermediate information.

Information systems

Although it has been studied by many specialists in different fields of activity, the information system does not have a unique definition, usually highlighting some or other of its structural or functional elements.

In this sense, we can study and analyze several approaches to this concept so that we can detach those common elements that give us an overview of what an information system means and involves.

On the one hand, according to AAP 6/2019, the information system represents a ”set of equipment, methods and procedures and, if necessary, personnel, organized to fulfill the information processing functions”[4]. On the other hand, the American military specialists define the information system as the ensemble formed by ”the entire infrastructure, circuits and information flows organized in a unitary conception, the personnel, all the components that collect, transmit, store, process, elaborate/process information and ensure their display and dissemination, in order to capitalize on the leadership process (command and control) and in the conduct of military actions”[5].

Thus, summarizing the opinions of different specialists, we can consider that information systems consist of specialized staff and structures, infrastructure and other essential elements that contribute to the collection, analysis and processing, storage and dissemination of information. All these elements represent the basis of the operations planning process in order to make the best decision to achieve the final objective or, in other words, to achieve the desired final state, ensuring the common operational image.

In this regard, I would like to emphasize that the information system should not be mistaken for those information gathering structures that support the process of planning and conducting operations. It includes, in addition to the intelligence system, the communications and IT system, i.e. not only the persons and structures that ensure the flow of information, but also the infrastructure necessary for its development. The information system consists of a complex set of specialized people and practical activities, technical equipment for gathering information (including through sensors), communications, storage, processing and display of information, software, databases and procedures, aimed at identifying the needs of information and how to satisfy them for the information assurance of the management processes (command and control), including the transmission of decisions to the subordinated operational levels (echelons).

Part of the information system, we identify as we mentioned the intelligence system, and in it we discuss the intelligence activity with a particularly important role in the process of planning and conducting military actions. The intelligence activity provides decision-makers with all that data and information about the enemy and the confrontation environment necessary for making the best decision to carry out the military mission. When we talk about the intelligence activity we refer not only to the activity carried out by the specialized structures in this domain, but also to the activities carried out by our own elements that can provide useful data to the process of planning and permanent updating of the situation. Knowledge of the confrontation environment and a more realistic picture of the enemy’s actions are essential in guaranteeing success in the battle space.

I consider that the continuous update and upgrade of the communications and IT system is a priority in order to support the growing need for information, data circulated in them, and development trends. All these can be highlighted by a brief presentation of the information and tactical communications systems adopted by the armies of some NATO member states, some of which I will present in the following lines.

The U.S. Army has a system that replaces the old systems, at least tactically. Named ”Warfighter Information Network-Tactical / WIN-T”[6], it is a communications system designed to provide support for C4ISR systems, secure voice, data and video communications. WIN-T has an infrastructure based on terrestrial communications, relying on high-capacity radio communications lines, network services and cellular services. WIN-T has been designed to perform missions in a variety of locations, at different echelons, to ensure quality communications regardless of tactical field conditions. WIN-T provides communications networks (satellite and terrestrial) and services that allow the exchange of information in order to carry out the mission.

During these years, the British army is also undergoing an intense process of modernization in terms of communication systems. Thus, Cormorant is the name of the project for the realization of the large-area communications network in the theater of operations, being a network that can be deployed quickly. Cormorant ensures a tactical internet capability from unit level to operations theater/strategic commander level. The main facilities offered are the following: a large area network for deployed forces, (the network can be deployed quickly by air and is tactically mobile), modular communications system, interoperability with networks of categories of armed forces and strategic support for joint forces of any size.

The Falcon communications system has replaced the previous Ptarmigan system and is a new generation of tactical communications system. It will provide secure and secure voice and data services, and the technology behind the system will be ”All over IP” – all via the Internet protocol. ”The key platforms will be Wide Area Switching Provision (WASP) a node with up to six radio relay links that will allow connection to Bowman local area networks and backup connections (via SATCOM) to the fixed communications system and Command Post Support (CPS) – Points which will be configured on different dimensions, depending on the missions that British forces will carry out”[7].

The BOWMAN communication system uses the latest trends in radio and IT technologies to meet the growing needs of services. It is designed to provide an integrated digital communications network, interfaced with higher-level systems and networks such as ISDN, Skynet V, Cormorant and FALCON.

”Bowman is a digital system that provides safe and secure voice and data communications, as well as an integrated global positioning system (GPS)”[8]. Bowman will provide an advanced tactical communications system using VHF, HF and UHF radio communications. It is the main means of command and control at the lower echelon of command of the brigade in ground operations. Its main features include secret communications, the ability to operate while moving platforms, independence from fixed infrastructure, light weight and size and simplicity. Bowman will also provide an integrated system of secret tactical communications for the ground component of the three categories of armed forces that participate in or directly support ground or shore operations. The system provides a wide range of services, especially at the level of the brigade and its lower echelons, including services that had not been available in the tactical environment. These services include secret communications of messages, voice and data down to the section level and a better knowledge of the tactical situation and the location of military units.

Among the armies that joined NATO a little more recently, we note the integrated communication system of the Polish army JASMINE. The technology implemented in the JASMINE system is fully compatible with the equipment in the stationary networks based on the TCP/IP protocol. The system is a reliable solution for control points at any tactical level, can connect older production equipment being fully interoperable with Cisco technology and is produced almost entirely in Poland. ”The system is available in two variants: mobile – mounted on specialized vehicles and portable – mounted in transport containers, each piece of equipment can be deployed elsewhere. The capabilities of the JASMINE system are: the possibility of developing separate data networks for the various functions of the control points, connection to infrastructure networks, information secrecy, IP applications for voice, data and video”[9].

The system consists of the following component subsystems:

- JASMINE Web Portal – allows the creation of Common Operational Picture – COP, integration of other systems, and facilitates user access to the JASMINE C3IS subsystem;
- C3IS JASMINE – battle space management software solution (example: creation of Common Operational Picture – COP);
- HMS JASMINE – Headquarter Management System, with the two components, fixed and mobile, consisting of data communication platforms dedicated to serving command points, to ensure C4I systems at the operational and tactical level;
- BMS JASMINE – Battlefield Management System for Battalion, Company, Platoon and Section, dedicated to terrestrial, air and maritime platforms at tactical level all components being of the ”on board” type;
- VIS JASMINE – Vehicle Intercom System, which ensures intercommunication at the level of platforms in IPv6 technology, with components such as ”on board”;
- DSS JASMINE – Dismounted Soldier System, which ensures their communication and integration needs at the soldier level; Information Exchange Gateway (IEG) JASMINE, is the software and hardware solution for secure exchange of information between different security domains;
- Combat IDentification Server CID JASMINE (CID JASMINE) – subsystem consisting of software and hardware modules that mainly provide the service of automatic updating of warnings on the situation of forces and monitoring of actions – situational awareness (SA) by identifying own and allied forces, exchange of data in the area of operations, security of own forces;
- JASMINE Management System (JMS), subsystem intended for the maintenance, management, monitoring and software configuration of all equipment that make up the JASMINE system.

The information component of the battle space

Regarding the information component of the battle space, my point of view is that it has involved many transformations in recent times, playing a key role in the process of planning and conducting military actions. It contributes substantially to the determination and provision of those essential issues to commanders and staffs for planning as close to reality as possible so that the fulfillment of the mission can be achieved with as little loss as possible and in a short time. Establishing and satisfying information/intelligence requirements as accurately as possible provides the staff and the commander with that relevant picture of what is happening and is likely to happen on the battlefield so that they can make the most appropriate decisions in a timely manner.

A major concern of military structures in operations, regardless of their level, is to obtain the information advantage that creates those conditions necessary for success on the battle space, avoiding, as far as possible, losses of any kind. Studying and analyzing the literature, we can say that there are three levels of information advantage, namely: information superiority, information dominance and information supremacy. I believe that in order to understand the three levels, we should start from their simple definition according to the Explanatory Dictionary, and then see their applicability in military operations.

Thus, superior means ”which is of better quality, which is distinguished by special merits. Superiority = State of that which is superior; the fact of being superior”[10]. At the same time, to dominate has the meaning ”to impose oneself by number or intensity; to predominate, to prevail. To prove clearly superior to the opponent. Domination = The act of dominating, exercising one’s influence or dominion; power, dominion, influence exercised over someone or something”[11], and supremacy presupposes ”absolute superiority united with authority and power; dominant position; preponderance”[12].

Obtaining and maintaining any of the three levels are based on both a high-performance information system, with staff and specialized structures in the intelligence field, but also on the infrastructure so that the intelligence cycle is as complete and short as possible. At the same time, we cannot ignore other aspects related to culture, religion and people’s behaviors.

The definition of one of the three levels can be made taking into account:

- the possibility to collect a large amount of information from several sources and environments (political, military, social, economic, electromagnetic, computer, religious, nature), about the enemy and its own troops, both from the area of responsibility and from the of interest, necessary for the decision-making act;
- reducing the likelihood of using false or null-value information by adopting efficient collection and authentication techniques and procedures;
- the performance of the technique for collecting information and its ability to take information in a fixed format (images, sounds), which makes it possible to transmit them in the form of data and their automatic processing;
- the ability of communication systems to convey the entire flow of information with high authenticity and in a short time;
- the degree of protection and security of data and information on own troops and their actions;
- the ability of the governing bodies to use that information, to concretize it in the form of decisions, so as to advance the probable actions of the enemy”[13].

Most frequently, in military operations, the level of information superiority is obtained, which represents ”the ability to carry out all the processes of the information cycle in a shorter time than the opponent with a higher degree of security”[14]. We discuss about information superiority when we can evaluate the information systems of the parties involved. In this situation, the intelligence cycle of the one who has information superiority is superior in results of the other, i.e. collects, processes and disseminates in the shortest possible time a larger volume of information, which proves to be truthful and, especially, useful to the decision making process.

Military analysts highlight the role of information superiority in the context of qualitative changes aimed at increasing information processing power, distributed processing, increasing software processing capacity, achieving knowledge superiority through doctrines, training, education and use of higher knowledge tools, holographic display, visual means of making smart decisions[15]. All this will increase the speed of decision making and reduce the duration of the complete decision-making cycle, with leadership tending to be achieved in real time at all levels, from days and hours to minutes and seconds by working simultaneously, transforming leadership from a punctually process in a continuous one.

Thus, the main directions of action that we have identified in this regard are:

- training and education of the personnel specialized in collecting and processing information;
- elaboration and updating of specialized doctrines, regulations and manuals;
- adapting intelligence structures according to requirements to ensure flexibility, mobility and freedom of action;
- permanent modernization of the equipment used according to the requirements of the battle space;
- permanent updating of techniques, tactics and procedures specific to the collection, processing and dissemination of information;
- use of an efficient and fast reporting system.

Referring to the second level of information advantage, information domination refers to the situation where the information system of one party is far superior to the other and “represents the degree of information superiority that always gives the owner the opportunity to use its own information system to obtain operational advantages in the conflict or to control a certain situation, simultaneously with the reduction of the possibilities of the opponent to use the necessary information to him”[16].

Also, the information supremacy represents ”the maximum level of the information advantage that always offers the possessor the possibility to un-hinder its own intelligence cycle, with maximum results, simultaneously with the control and influence of all information processes of the opponent, outside his science, in order to achieve his goals with minimal losses”[17].

I believe that information supremacy, being the maximum level of information advantage, is very important because dominating information certainly ensures success in battle. We are talking, in this situation, of a clearly superior advantage over the enemy, a situation in which the enemy is unable to go through his own intelligence cycle which will clearly affect his entire process of planning operations which leads to the inability to fulfill its mission or achieve the ultimate goal.

Yet, from my point of view, we need to act gradually in terms of the information advantage so that we gradually ensure a certain level of it and act to reach the next one. I consider that information supremacy is rather a desideratum, it is very difficult to achieve and, especially, to evaluate, as there is a relatively sensitive barrier between the second level of information domination and that of information supremacy.

There are several distinct types of threats in today’s security environment. Each represents a different challenge requiring a specific “way of war” and consequently different concepts, doctrines and force structures, as well as different approaches in terms of intelligence activity.

In this area, many changes have taken place in the last period of time in order to adapt to the new types of threats that make their presence felt and have effects in the contemporary security environment. This new approach to intelligence activity, developed correctly in action, ensures the asymmetric advantage in the context of any challenge, whether violent or nonviolent, states or organizations, immediate or long-term.

The component of activities focused on precise elements should be strengthened in future intelligence work. It is very important to note that the new approach places great emphasis on history and the open source network. The analysis of history lessons is fundamental for the information activity.

Conclusions

So, in recent decades, we have witnessed a diversification of the types of threats to national and even international security. What until recently was considered a template has undergone substantial changes and we now face multiple and increasingly diverse threats. Obtaining the most complete and timely information has become essential in the battle space to make available to decision makers, regardless of level, everything necessary so that the decision is as correct as possible and adapted to the reality of the battle space.

That is why paying special attention to information systems in the process of planning and conducting military actions is essential. And we refer here, as it appears from the analysis carried out in this article, not only to the intelligence system and implicitly the intelligence activity carried out by the own intelligence structures and not only, but also to the infrastructure necessary to complete the intelligence cycle in time as short as possible.

Obtaining a high level of information advantage in the battle space offers us, practically, that upper hand of being constantly one step ahead of the enemy, so as to accomplish the mission with as few losses as possible, regardless of their nature.

NOTES:

[1] Sun Tzu, *Arta războiului,* Cartex Publishing House, 2018, p. 42.

[2] Ion Roceanu, *Sisteme C4I comandă și control, comunicații, computere și informații*, National Defence University Publishing House, Bucharest, 2004, p. 9.

[3] *Ibidem*, p. 10.

[4] *AAP6 (2019), NATO Glossary of Terms and Definitions*, 2019, p. 67.

[5] *FM 101-5-1, Termeni şi simboluri operaţionale*, Land Forces HQ, SUA.

[6] https://www.en.wikipedia.org/wiki/PM_WIN-T#WIN-T_Increment_1, accessed on 15.04.2020.

[7] https://www.army.mod.uk/equipment/communication-and-surveillance, accessed on 15.04.2020.

[8] *Ibidem*.

[9] https://www.teldat.com.pl/en/offer/products/systems/165-jasmine-system-of-the-systems.html, accessed on 16.04.2020.

[10] www.dexonline.ro

[11] *Ibidem*.

[12] *Ibidem*.

[13] Ion Roceanu, *op.cit*., p. 15.

[14] L. Armistead, *Information Operations: Warfare and the Hard Reality of Soft Power*, Brassey’s Inc. Publishing House, Washington, DC, 2004, p. 17.

[15] *Ibidem*, p. 18.

[16] *FM 3-13, Information Operations*, Headquarters, Department of the Army, 2016.

[17] Ion Roceanu, *op.cit*., p. 20.

REFERENCES

*** AAP6 (2019), *NATO Glossary of Terms and Definitions*, 2019.

*** ADP 2-0 *Intelligence*, Department of the Army, July 2019.

*** FM 101-5-1, *Termeni şi simboluri operaţionale*, Statul Major al Trupelor de Uscat, SUA.

*** FM 3-13, *Information Operations*, Headquarters, Department of the Army, 2016.

*** *Carta albă a apărării*, București, 2017.

Armistead L., *Information Operations: Warfare and the Hard Reality of Soft Power*, Editura Brassey’s Inc., Washington DC, 2004.

Roceanu Ion, *Sisteme C4I comandă și control, comunicații, computere și informații*, National Defence University Publishing House, Bucharest, 2004.

Sun Tzu*,* *Arta războiului*, Cartex Publishing House, 2018.

https://www.army.mod.uk

http://www.dexonline.ro

https://www.en.wikipedia.org/