Laurian GHERMAN
Cosmina Oana ROMAN
Marcel HARAKAĽ

ELECTRONIC WARFARE IN THE INFORMATION AGE

Liptovský Mikuláš
2015

Authors:

© Dr. Eng. Laurian **GHERMAN**
Cosmina Oana **ROMAN**
Assoc. Prof. Eng. Marcel **HARAKAĽ,** PhD.

Reviewers:

Eng. Michal **TURČANÍK**, PhD.

The Armed Forces Academy of General M. R. Štefánik, Liptovský Mikuláš, 2015.

ISBN 978-80-8040-512-0

CONTENTS

1 WARFARE AND THE INFORMATION AGE

1.1 The transition to the Information Age

For a better understanding of the difference between the Information Age and the Industrial Age, the aspects that have undergone radical changes need to be first identified. One can easily see that the technological development in the past years has caused an exponential increase in the capability to collect, process, disseminate, and use information.

The most important technological advance is associated with the spread of information.

Technological advances have enabled information to be spread over long distances, which has fostered a better cooperation between individuals and worldwide organizations. Yet, in order to understand what the Information Age is, one needs to study its beginnings, which are deeply rooted in the Industrial Age.

It is only fair to say that the studies of MICHAEL FARADAY (1791 – 1867) in the field of the electromagnetic induction constitute the laying foundations of the technological progress recorded in the Information Age.

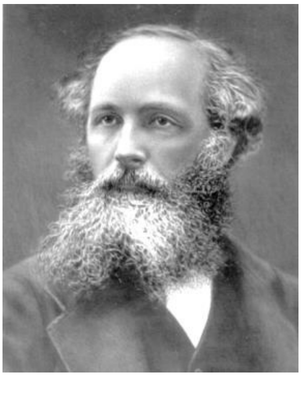


Fig. 1 James Clerk MAXWELL

The understanding of the way in which the magnetic field influences the electric field and viceversa is one of the pillars of the Information Age, i.e. transmission of information over long distances.

This technical capability was possible owing to studies carried out by JAMES CLERK MAXWELL (1831-1879). In his book *A DYNAMICAL THEORY OF THE ELECTROMAGNETIC FIELD* from 1865, Maxwell demonstrated that electric and magnetic fields travel through space at the speed of light as waves.

For the first time in history, the existence of the electromagnetic waves had been demonstrated theoretically.

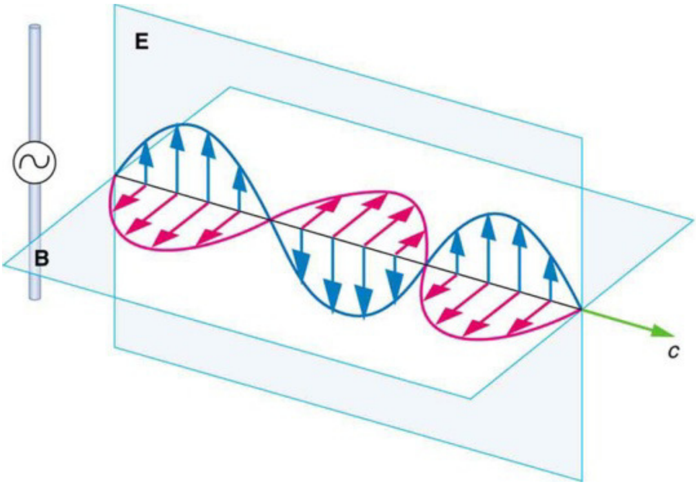


Fig. 2 Magnetic (B) and electric (E) fileds form an electromagnetic wave

The next step was made by HEINRICH RUDOLF HERTZ (1857-1894), who demonstrated in practice how electromagnetic waves were produced.

The discovery of the electromagnetic waves made it possible for the transmission of information over long distances at vey high speeds (the speed of ligh), which virtually meant instantaneous transmission of information

But this alone was not sufficient to make the transition to the Information Age possible. The second factor that did enable this was the digital revolution. In the second half of the 20th century, digital computers allowed for the information to be generated, multiplied, stored, and transmitted at low costs and in high quantities. This has resulted in the information becoming increasingly cheap and available to more and more people.

For a better understanding of the impact of Information Age on military organizations, a series of specific aspects need to be carefully analysed.

Therefore, for a military organization to be able to ensure victory against opponents, high quality weaponry became a necessity. The development stages of such weaponry can be accurately identified throughout history.

Around the mid-20th century, the weapons systems' rate of development decreased. It had reached a point when the characteristics of the weapons systems used by various military organizations were comparatively similar.

Let us consider, for instance, several types of aircraft. We shall see that their maximum speeds are very close. It was noted that attempts to increase the speed resulted in costs being so high that they could no longer be covered.

This is the reason why Air Forces opted for aircraft reaching speeds around 2 MACH. For higher speeds, as in the case of SR 71 *BLACKBIRD,* the efficiency of the production and operating costs was below threshold. The development of other physical characteristics reached a limit, too.

Fig. 3 Lockheed SR 71 Blackbird

A closer look at the maximum flight speed will clearly point out the compromise required to achieve the best performance.

U2 Dragon Lady best epitomizes this. Given the fact that these physical characteristics are comparatively similar in all aircraft used by various Armed Forces, finding the way to achieve air supremacy became a necessity.

One direction of development from the same period of time, i.e. mid-20th century, was to reduce the effective reflexion surface for the electromagnetic waves in military aircraft.

Fig. 4 U2 Dragon Lady

Thus, a new generation of STEALTH-like weapons was born. Regular radar systems could only detect them with difficulty.

The same arguments underline other categories of military equipment as well. This direction of development secured the achievement of air supremacy up to the moment when it was demonstrated in practice that these aircraft could also be taken down by antiaircraft missile systems adapted to the new realities.At this stage of development, with scientific discoveries being applied to the military field, it seemed that the way to secure victory was to increase the numbers (in terms of personnel and military equipment).

Consequently, the seeming answer was: a large number of aircraft, tanks, troops, etc. However, this meant huge operating expenses, which later led to the same situation, when boosting the physical performance of weapons was attempted.

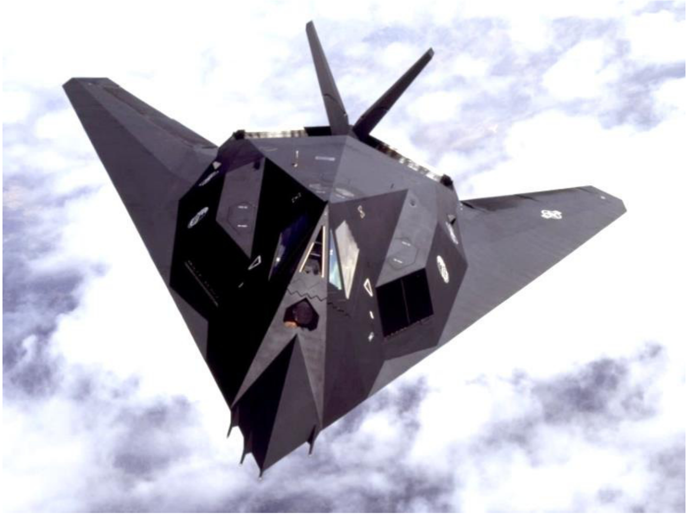


Fig. 5 Lockheed F117 Nighthawk

But in mid-20th century, something remarkable occurred: the digital revolution. Since the development of digital devices is exponential, it is the digital revolution that fostered the transition to the Information Age.

In 1965, GORDON MOORE noticed that the number of transistors in an integrated circuit doubles approximatively every second year. Based on this observation, he predicted that this development trend will continue. This prediction is now known as the MOORE's law. The MOORE's law can also be applied to such digital systems performance as: calculating speed, information storage capacity, transport capacity of networks, etc.

This unprecedented development in digital technologies caused major changes in the society.

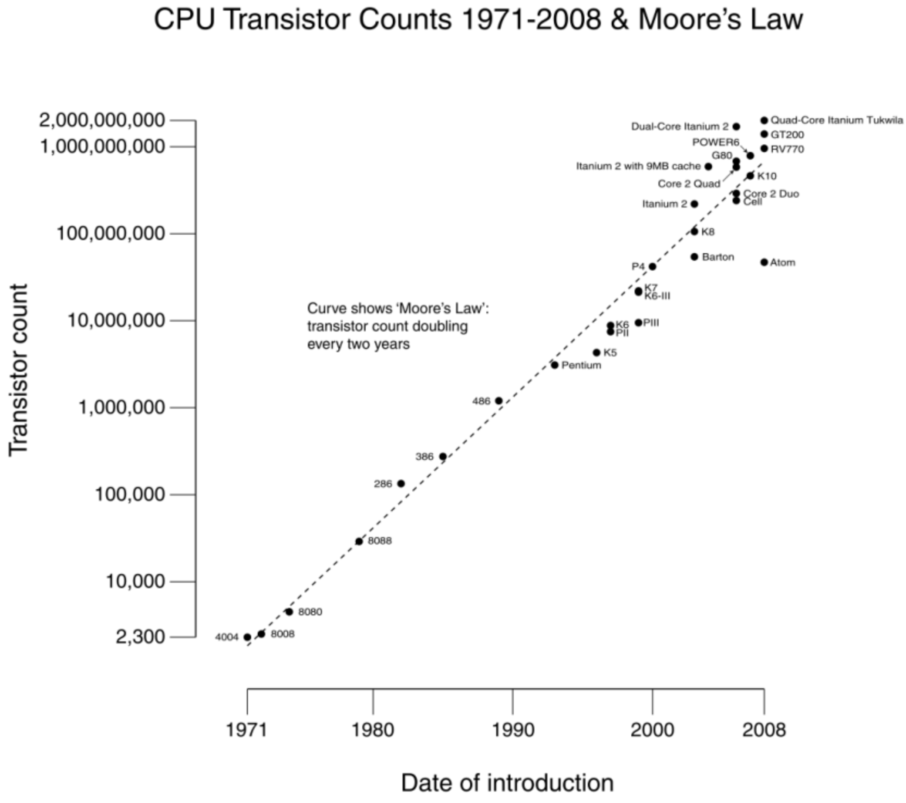


Fig. 6 Moore's Law

These transformations affected military organizations as well, which were, thus, forced to switch from concepts specific to the Industrial Era to approaches characteristic of the Information Age.

1.2 Information – explanatory aspects

In order to understand how information affects the ability to carry out military operations, three domains need to be taken into account:

- Physical domain;
- Information domain;
- Cognitive domain. [1]

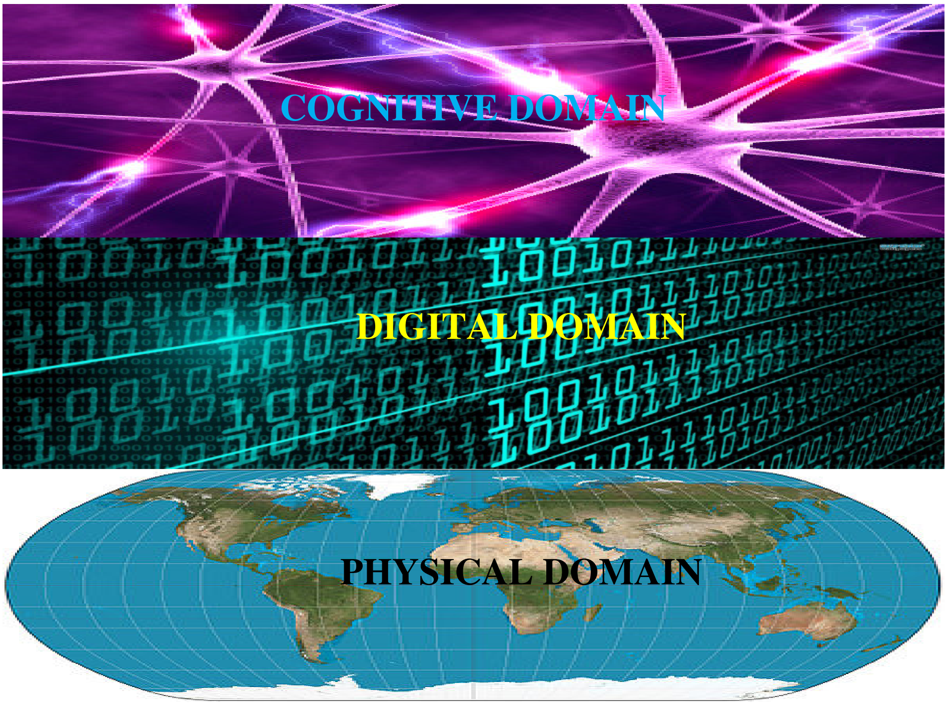


Fig. 7 Domains of action for military operations

The physical domain is the place where those situations that the military try to influence exist. It is the domain where attacks, protection, and manoeuvres occur, be it on the ground, by sea and in space. It is the domain where physical platforms and the communications networks that connect them are located.

Comparatively, the elements of this domain are the easiest to quantify, which is why, traditionally, the fighting power has been measured particularly in this domain. There are quite a few analyses and models, in which the physical domain is charaterised as reality or fundamental truth.

Important indicators used to assess the fighting power in this domain include mortality and survival rates.

The Information domain is the space where information exists. It is the domain where information is created, manipulated, and transmitted. It is the domain that allows for information to be communicated among fighters. It is the domain where the command and control of the armed forces is exerted. The information that exists in the Information domain may or may not reflect the reality. For instance, a sensor that observes the real world produces data that exist in the Information domain. Except for the direct observation of the sensor, all the information about the world travels through and is affected by the interaction with the Information domain.

It is only through the Information domain that communication with the others is possible (one exception could be telepathy).

Consequently, in order to allow a force to generate fighting power in response to offensive actions carried out by an adversary, it is becoming increasingly important to protect and defend the Information domain.

In all fights relevant to achieving information superiority, the Information domain is the most important.

The cognitive domain forms in the participants' mind. This is the place that allows for decisions to be taken, where perceptions, awareness, understanding, beliefs and values coexist.

This is the domain where, at present, numerous battles and wars are lost or won.

This is the domain of the attributes care can create an untouchable army: the leadership, morale, unit cohesion, level of training and experience, situational awareness, and public opinion.

It is the domain where doctrines, tactics, the understanding of a commandant's intentions, techniques and procedures exist.

There are numerous books on this domain, and the essential characteristics of this domain have remained relatively constant ever since SUN TZU (544 – 496 BC) wrote *THE ART OF WAR*.

The attributes of this domain are extremely difficult to quantify, and every sub-domain (every individual mind) is unique.

All the components of the cognitive domain travel through a filter or a lens which is characteristic of human perception. This filter comprises an individual's perception of the world, the level of personal knowledge with which a person contributes to a situation, the experience, training, values and individual abilties (intelligence, personal style, perceptive abilities, etc.). Since these lenses which represent human perception are unique for each and every individual, then it means that individual cognition is also unique.

Therefore, there is only one reality, or a single physical domain. This thing is converted into selected items, information and knowledge related to the systems in the information domain.

Through training and exchanges, similar cognitive activities aimed at decision making in the military are attempted. However, each individual stays unique in their own way, notable differences existing among the individuals belonging to different generations, countries or services, rather than those from the same unit or service.

Given the fact that within the cognitive domain the differences between the personnel of various military organizations are not as significant so as to secure victory in the Information Age, it is necessary to look for the prerequisites of victory elsewhere. Along the time, when progresses made in the physical and information domains were similar in all military organizations, it was the difference in the cognitive domain (the quality of the combatants) they secured victory on the battlefield.

As previously shown, at the beginning of the information era the advances in the physical domain reached a threshold which resulted in victory being determined by advances in the Information domain.

But in order to understand the role of information within military organizations, it is necessary to examine first their role along the years.

Information has always been at the heart of military operations. Throughout history, military leaders have acknowledged the key role played by information in achieving victory on the battlefield. Commanders have constantly tried and, occasionally, succeeded in gaining a decisive information edge over their adversaries.

The works of SUN TZU and CARL VON CLAUSEWITZ (1780–1831) reflect the great importance attached to information in wartime. In his 2500 years old writings, SUN TZU underlined the importance of being aware in wartime:

„If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

CARL VON CLAUSEWITZ's works are well known for the famous fog war concepts:

„All action takes place, so to speak, in a kind of twilight, which like a fog or moonlight [...] War is the realm of uncertainty; three quarters of the factors on which action is based are wrapped in a fog of greater or lesser uncertainty. The commander must work in a medium which his eyes cannot see; which his best deductive powers cannot always fathom; and with which, because of constant changes, he can rarely become familiar."

As a result of these permanent characteristics of war, military organizations have been designed for centuries to adjust the lack of valid information, this being the way in which the fog characteristic of was is dealt with.

Fog is represented in its entirety by uncertainty, more specifically by the uncertainty regarding information about location, capabilities, and kinds of intentions.

Until recently, a commander could not have an accurate picture in real time of his own troops, let alone feel comfortable about the information he had on the enemy's position and intentions. The conflict refers to all the errors that appear while the forces'synchronization plans are in progress or even to carrying out the simplest tasks.

Some of these types of misunderstandings can be attributed to fog, others to poor quality communications, or even to a lack of common knowledge.

In order to combine this issue, decision making process in wartime entails an extremely high error cost. Consequently, it should not surprise us that the notions of operations, organizations, doctrines, and training have always been concerned with reducing the risks and effects associated with fog and conflict.

Taken together, these war characteristics have shaped our traditions, our military culture, as well as our thought. Deviation from these norms will be difficult, and will require a high level of difficulty to prove that the new way is not only much better, but also robust. Recent technological advances offer the opportunity to reduce the fog and conflict. Anyhow, despite all the past and future progresses, a significant amount of residual fog and residual conflict will persist. The nature of this residual uncertainty is still unclear, and its implications are not fully understood. However, there is a possibility to reconsider the best way to handle the persisting fog and conflict, and this think is likely to have deep implications for the military operations and organizations.

In Fig. 8 the relation between the amount of fog and conflict, and the synchronizing level are shown, which can be conveniently obtained in military operations, a fact which is directly associated with efficiency.

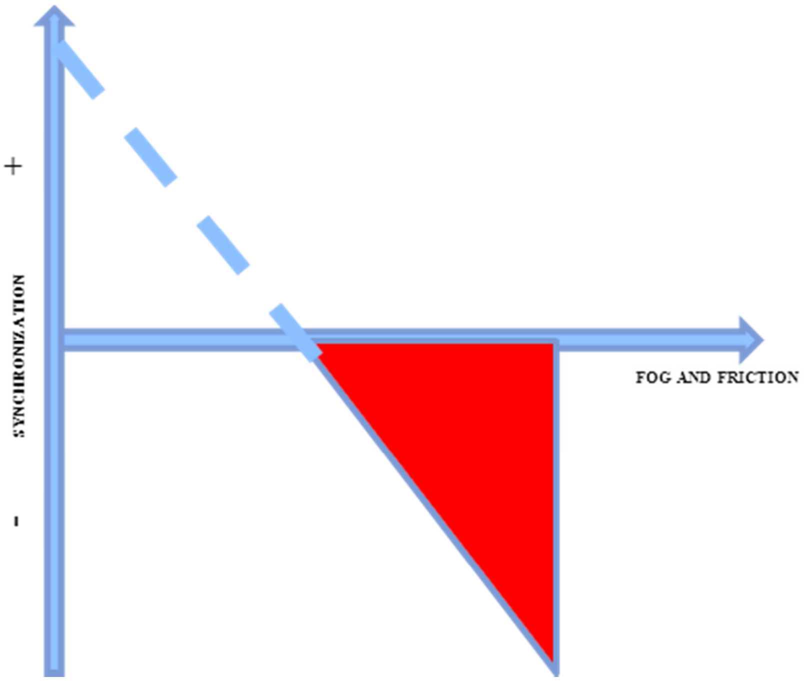


Fig. 8 The link between fog, conflict and synchronization [1]

For approximately all the important moments in our history, the battles was in various parts of the dark area, the worst parts of the space (bottom right) being avoided.

The Information Age gives the opportunity to move to the white area. It should be acknowledged that the ability to reduce the war fog and conflict in not only limited, but in many cases, impossible.

Owing to such missions as those in Somalia and Bosnia, we have been witnessing the complexity of the 21st century, and thus, the limited ability to collect, process, and distribute information.

Consequently, in order to examine the role played by information in wartime, it should be clear not only the way in which the advantage given by information is created, but also how residual uncertainty, which undoubtedly exists, can best be handled.

Those who claim that we are fully aware of or that we will eliminate the war fog are, indeed, false, if not dangerous, prophets.

They are characterised as such not only for the obvious reason that they can influence courses of action in a totally ineffective direction, but also because they ruin the ideas for making the best use of developing information and network connection capabilities, which could, in fact, provide real opportunities to improve military effectiveness.

Impacting directly on the considerable degree of uncertainty, the limited abilities to efficiently communicate on the battle field, and the extremely high cost error, the information flow has been, throughout the entire history, connected to the command structure and specific behaviours on the battle field.

Traditionally, commanders have always looked to counteract uncertainty by using risk reducing approaches, of which the risk of being taken by surprise was the most important.

Great achievements were frequently made on the side with the fewest errors, rather than the imaginative or daring one. Anyhow, the price paid for evading the fog and conflict has been high, as these solutions carry some significant advantages.

The ability to tap into opportunities, as well as to react is absent, and therefore it is not possible to easily adapt to changing situations. Also, existent resources are insufficient.

Briefly, these traditional adaptations are 180° not in line with the attributes wanted by the military men of the Information Age.

But technological advances are not the only ones defining the Information Age. It is extremely important how these new technical capabilities are used. This allows individuals and organizations to create new values and methods.

In leading an armed conflict, the greatest emphasis is placed on organisational concepts. These new forms of organization involve changes in the way in which authority is exerted and control is maintained.

In numerous cases, these new forms of organization have overpassed the more traditional competitive forms.

One of the characteristics of these new forms of organization, which is of great importance for military organizations, is the increasing ability to adapt to a dynamic environment.

The virtual nature of these organizations is equally important, as they offer the ability to get together in real time, to minimize the need to move (instead of personnel, it is information that is transferred), and to compress time by performing operations 24 hours a day, 7 days a week.

The information and communication explosion in the technology field has significantly harmed the information economy.

One important aspect that has changed the information economy is the Internet, which best be explained through the concept of information abundence and access („Richness and Reach”).

This concept of digital wealth was defined as a measurement for the overall quality of information, whereas the information access as a measurement for the degree of information spread.

Historically speaking, it was necessary to choose between an exchange of information with a very limited range of action (such as, face-to-face talks supported with graphs, maps, etc) or an exchange of restricted information that has a much wider range of action (memos, etc.).

This choice was rather forced as, in the past, the economy of information has imposed an inverse relationship between the abundence of information that could be exchanged and the number of people with whom this information could be exchanged. This inverse relationship can be considered a compromise, as illustrated in Fig. 9, where a clear delimitation between the possibilities offered by the Industrial Age and the Information Age can be shown.

The key variables that influence the form and location of this curve are the highest level achieved at the respective moment (state-of-the-art) by information technology, and they lie at the heart of economy.

As soon as individuals and organizations have become increasingly capable of widening the access and range of action, they have started to focus on the quality of the access possibilities, as well as the quantitative aspects of access.

Therefore, the quality of interaction was added to the quantity / access construction (Fig. 10).

Thus, individuals and organizations have managed to provide all the three characteristics:

- High quality information;
- That can be easily diseminated by those who need it;
- In a way that facilitates exchange.

To illustrate the progress recorded by the quality of information, the nature of the exchanges used in military operations, which take place between and among the entities on the battle scene, need to taken into account.

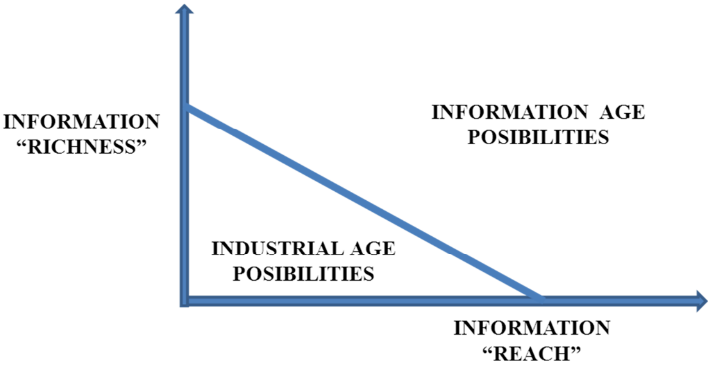


Fig. 9 The relation between quantity and information access [1]

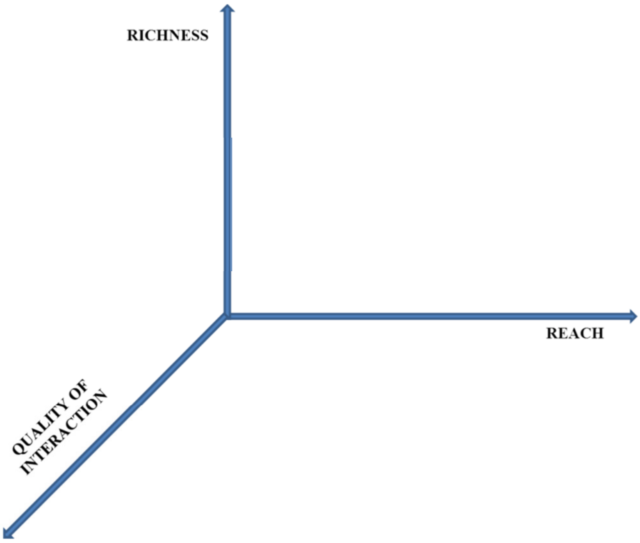


Fig. 10 The characteristics of information [1]

Given the advance of the state-of-the-art information technology, military communications have progressed from athletes and smoke signals, to the telgraph, the radio, the telephone, video conferencing, and all these advances fostering a completely functional, collaborative working environment.

As for the opportunities of the Information Age, we are refering to the ability to make the transition to a new part of the three dimensional areas presented in Fig. 10, which allows military organizations for the opportunity to significantly improve the key connections in the value chain, which closely connects information technology to mission effectiveness.

Military organizations now have the advantage of greatly improving their ability to exchange information (widening the range of actions).

This can be achieved because nowadays technology gives organizations the possibility to distribute and share information without seriously degrading them in terms of abundence.

Improvements in the ability to spread the information will contribute to improvements in the ability to generate and maintain common awareness, which, in turn, together with an increased ease in collaboration (the quality of interaction), will contribute to improving synchronization.

Thus, the progress in the information age which results in improved capabilities in terms of wealth, access and digital interaction space will affect the cognitive processes, which will reflect in the level of receptiveness, adaptability and flexibility.

These competences will provide for a new source of competitive advantage in the Information Age.

1.3 The Industrial Age Legacy

The network centric warfare is one of the types of wars used during the Information Age. This is a type of war that can and should be seen as a disruptive innovation because its key key attributes and apects disrupt nature. For instance, the information exchange and collaboration disrupt the existing decision making processes, as well as the organizational authorities and values.

To understand the way in which military organizations have adapted to the challenges of the digital age, it is necessary to understand how the command and control concept (C2) has changed in the Industrial and Information Ages.

C2 is a military term used to describe personnel and resources management.

Command represents the responsibility to use available resources, to organize, coordinate, and lead military forces in order to accomplish assigned missions.

Also, it includes the responsibility for the health, wellfare, morale, and discipline of the personnel under command.

Control stands for indentifying measurable indicators which can establish to what extent the command has fulfilled its responsibilities in order to implement corrective measures.

It is, therefore, obvious that the C2 term encompasses all the three domains, physical, information, and cognitive. Sensors, systems, platforms, and facilities also exist in the physical field. Information that is measured, analysed, displayed and stored exist in the information domain. The perception and understanding of what this information stand for exist in the cognitive domain. In the industrial age, competitive military organizations have adopted six types of command and control systems.

Depending on the level of centralisation, ranging from the most centralised to the least centralised, these types of C2 can be divided into:

- Cyclic;
- Interventionist;
- Problem-Solving;
- Problem-Bounding;
- Selective control;
- Control free. [2]

The cyclic model of C2 is the most centralised and consists of transmitting detailed orders from the highest command echelon, at regular intervals. This model is efficient when:

- Communications lines cannot ensure the transmission of a greater amount of information;
- The coordination of several types of units is necessary;
- Commanders at lower levels of command are not able to act independently (due to lack of information or training), and thus are forced to carry out received orders without using their initiative.

This model is efficient when there is time for the information to be gathered, transmitted to the central command echelon, and analysed, in order for best decisions to be taken, detailed plans to be drafted and sent to subordinates.

This model was successfully applied during WWI and it is representative of trench warfare. The same model was adopted by the Soviet armed forces in WWII owing to the lack of training of commanders at all inferior levels, in order to efficiently manage resourses and because communications lines were poorly developed.

The cyclic model was also adopted by the US Air Force when the Air Tasking Order was drafted, based on a 72 hour-cycle. In this system, air force missions were assigned based on the airplane tail number from the lowest level to the central command echelon. This approach allowed for the precise synchronization of all airplanes' missions.

The interventionist model is similar to the cyclic one, except for the communications lines which are more developed (they allow for the transmission of a greater amount of information), orders are transmitted at irregular intervals for an optimum use of potential opportunities.

During the Cold War, the soviet armed forces adopted this model because of improved communications lines and raise of the commanders' training level.

Although orders were still being transmitted from the central command, the units were trained how to act depending on the situation, and according to the best scenario.

For instance, to force the crossing of a river, the most efficient solution was identified, after which it was rehearsed by all the combat units.

The moment the combat unit received the order to force the crossing of a river, the previously rehearsed algorithm was applied.

The Problem-Solving model gives subordinates the possibility to creatively carry out received orders. However, the central command echelon sets intermediate objectives which need to be carried out at a certain interval and in a certain order.

Apart from the final objective, the central echelon sets the constraints that need to be respected in carrying out this objective. The manner in which both secondary and main objectives are carried out is the lower echelon commanders'duty. Virtually, they are tasked to solve certain given situations.

This type of command model was used by the US Army and US Navy in WWII.

The Problem-Bounding model consists in presenting the aimed objective, to which other minimum required information is added regarding the deadline, and the limitations imposed for carrying out the objective.

This model was used by the British armed forces during the Cold War. By training the personnel, it is possible to easily move from the intermediate objectives model to the limited actions model.

The selective control model gives lower echelons commanders even a greater responsibility. The Israeli armed forces have made the best use of this model. According to this model, lower echelons commanders have the freedom to take action in order to fulfill set objectives. The central command echelon intervenes only to tap into certain situations that might appear or to correct certain dysfunctional situations. Lower echelons commanders need to show discipline in order to carry out the orders received from the central command echelon. A strong level of trust needs to be developed among commanders at all levels of leadership.

According to **the Control free model,** the central command echelon sets the objective and provides forces under their command with the best conditions, information and required information.

This model was adopted by the German model in WWII.

An army corps had full authority to carry out objectives set by the central command echelon.

This type of model is less used given the high performance communications links between the commanders of various echelons.

The development of digital technologies has resulted in higher performance communications links and date transmissions between different components of the C2 system.

This has made it possible for any of the six command and control models in our Digital Age to be adopted by military organizations for a maximum efficiency in carrying out objectives.

The speed of data transmission between the various departments of a military organization has become increasingly important.

To understand how the working speed for available information can decisively influence whether victory is secured or not, it is necessary to analyse the OODA cycle (Observe, Orient, Decide and Act). This cycle was created by JOHN BOYD and it is applicable to all military conflicts, from individuals to organizations.

The four phases of the cycle allow for the sequential analysis of an armed confrontation. Initially, this cycle has allowed in the case of the combats during the war in Coreea to account for the reason why American pilots obtained more numerous victories.

By dividing the fight into the four phases of the OODA cycle, one can better see from where the combat advantage and, ultimately, the victory were gained in military confrontations.

The first phase of the cycle, **observe** refered to detecting enemy plane. In the second phase, **orient,** the pilot chose the position in relation to the enemy plane so he could move to ther third phase, **decide**.

In this stage, the pilot decided what he was going to do next (to shoot down enemy plane). In the fourth phase, **act**, the previously taken decision was put into practice. After this last phase, the cycle was resumed after a new evaluation of the situation.

By applying this analysis, BOYD noticed that the American pilots and their F-86 *SABRE JET* planes were superior to their enemies' in all the four phases of the OODA cycle.

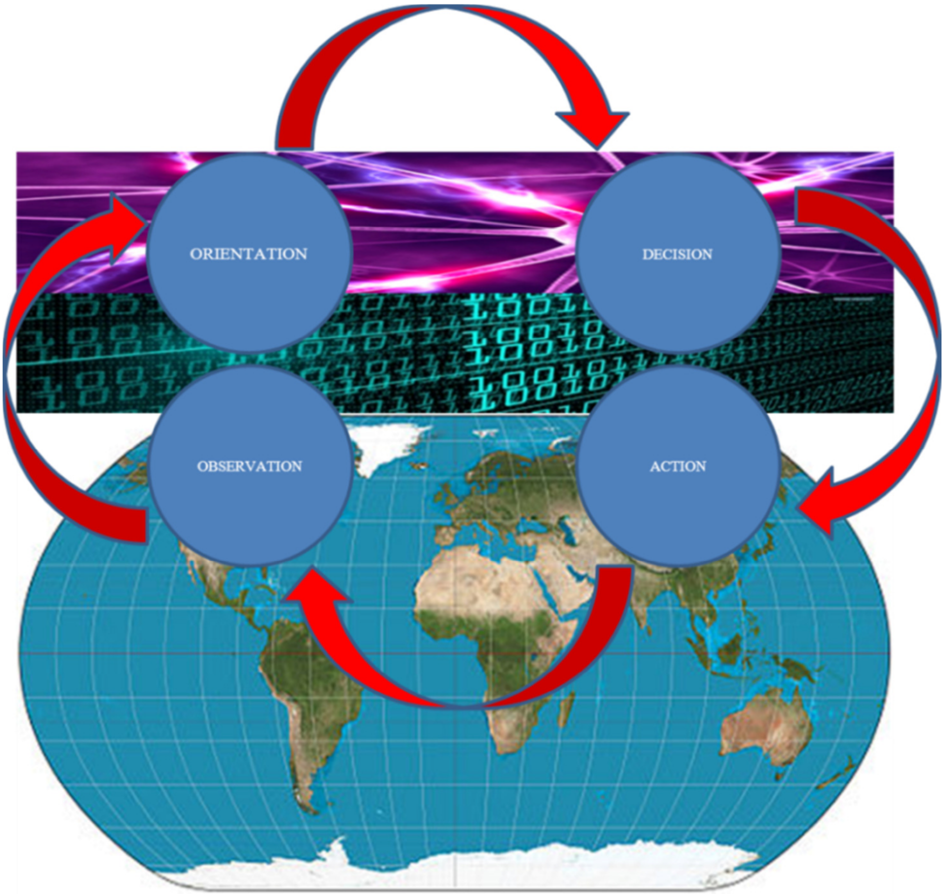


Fig. 11 The OODA cycle in air combat

As the American pilots went through the OODA cycle at a higher speed, they acted during the enemy's cycle, thus winning the air combat. This high speed was possible because during the observation phase, the information was more rapidly acquired by observing the physical environment, taking into account the position of the plane during the orient phase, while the decision to shoot down the enemy plane was being taken by the pilot.

As both planes had similar speeds, the decision was put into practice at a relatively equal speed.

Therefore, it can be seen that when the military systems in the physical domain share relatively similar characteristics, if one acts before their enemy, the chances to win in combat are the highest.

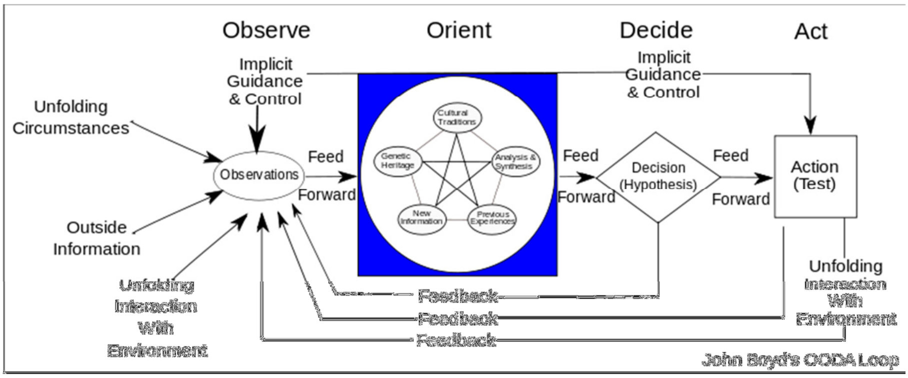


Fig. 12 The OODA cycle presented by John Boyd

Given the fact that the action speed cannot be significantly increased due to physical limitations, it is possible to increase the working speed by using the information during the other phases of the cycle (observe, orient, decide).

And the Information Age has made this thing possible. If during air combats in the Coreean war, the information was transmitted between the airplane systems and the pilot (and the American pilots were better trained), in the case of a military organization's components situated at large distances in space, the increase in the speed at which information travels is given by the existence of some high performance digital technologies.

Given the fact that a military confrontation can take place even between two military organizations, the same analysis method can be applied, except that the cycle has a more complex form, as shown by Boyd in 2001.

It has, therefore, been demonstrated that in the case of some military systems with similar physical characteristics, victory can be achieved when the OODA cycle's speed is higher, which allows for "getting inside the enemy's OODA loop".

Speed in the information domain can secure victory in the physical domain. The Information Age gives military organizations precisely those tools through which the speed in the information domain can be increased. When reaching this point, something absolutely unprecedented occurs within military organizations. This thing questions a military organization's fundamental principles, such as hierarchy and relations between individuals, structures, and processes.

The hierarchy and the relations within a military organization have been created, tested and improved throughout the history considering a certain speed in the information domain.

And by speed in the information age, I mean the speed for acquiring, storing, processing, multiplying and trasmitting the information.

As previously shown, in the Information Age there is an explosion of speed increase. The information age's tools allow for speed to be increased within the military organizations, yet the traditional structure of hierarchy becomes an obstacle in using the power of information at its fullest.

Decades of efforts have led to an increase in the interoperability of the communications systems. These processes have become faster owing to the changing digital technologies. The huge progress in terms of storage, processing power, and bandwidth has allowed for a higher distribution of data, information, and images.

Modernised sensors, new platforms, (from satellites to UAVs) and improved fusion algorithms, novel approaches possible thanks to a bigger processing power, have caused an increased awareness of the combat area and a reduction in the level of uncertainty in several contexts.

Tools such as videoconferencing or extended bandwidth to distribute a larger volume of information, if only as PowerPoint files, have boosted the level of undestanding, thus allowing for more varied decisions to be taken.

Similarly, decision processes are now faster and have resulted in a common understanding of what needs to be done, and an improved quality of combat management.

Perhaps the most difficult aspect regarding C2 in the Information Age is the way in which C2 organizations are modified. Military culture is deeply rooted in a structure that, functionally speaking, is divided into smaller parts in terms of combat components (responsibility divisons such as armoured vehicles, ground, air, sea and underwater artillery in naval wars) and in terms of group elements (personnel, operations, etc.). These divisions are confirmed by traditions, armament, and experience.

They represent an essential component of the military culture. Therefore, they will resist change.

Anyhow, the present organizational divisions are the end product of the information technologies and capabilities before Information Age.

For instance, the weapons platforms had, for generations, their own sensors or depended upon the five senses of the operators in service. In the Information Age, sensors can be disconnected from the weapon platforms and, quite frequently, even from the platforms with people on-board. Thus, the sensors can be placed in a dangerous place, while people are safe.

Organizationally speaking, the information from the sensors can become available to potential shooters, in safe positions. Under such circumstances, and especially when the need for a rapid reaction is crucial (the ever increasing mobile targets, the more accessible arms with terminals, etc.), the artificial distinction between the quality of intelligence (sensors) and the quality of operation (shooters) is pointless.

Since priorities have been established, and the criterion for aiming the weapons at targets is understood (including the quality of the information available according to which only correct targets are dealt with, and collateral damage is taken into consideration), the fewer the organizational barriers to collaborative planning and synchronizing of activities, the better. The changes within the C2 organizations are crucial for acquiring the benefits available in the Information Age.

This is to be expected, owing the cultural obstacles, and the high costs resulting from wrong approaches. The great difficulty in testing new methods of organization (identifying commanders and personnel that can undertake experimental approaches without creating problems regarding their current training and level of skills, identifying the facilities that can withstand such tests, etc.) has already emerged has a practical issue.

Finally, in any case, the full impact of concepts and technologies in the Information Age cannot be acquired without adequate changes within the C2 organizations and the collections of empirical data as part of structured war games, exercises and experiences.

As previously argued, human behavior is, simply, too complex to be shaped or dealt with by means of assumptions. The military organizations' solution to the challenges of the Information Age is the network centric warfare.

1.3 Network centric warfare

The network centric warfare concept has resulted from the civilian organizations' experience, which have successfully adapted to the Information Age. Those civilian organizations that failed to adapt have disappeared.

Without the development of new relations between people, components of the military organizations and processes, it is not possible to fully exploit the power of information.

The network centric warfare allows for combat power to be generated by the network connections between sensors, command elements and shooting systems.

This network allows for a unitary image of the battlefield to be created and distributed to all the elements in the network, which ensures self-synchronization between the various geographically dispersed elements in order for the intentions of the command structure to be carried out.

But in order for a new command structure to be created which would rise to the challenges of the information age, it is necessary to analyse how the actual structure has risen to the industrial era's challenges.

The principles underlying the development of a command system in the Industrial age are, as follows:

- Division;
- Specialization;
- Hierarchy;
- Optimising;
- Centralised planning;
- Decentralised implementation. [2]

Next, we are going to present the way in which each of these principles have influenced the structure of the control and command system in the Industrial Age.

Division – in the Industrial Age, the Latin proverb *„Divide et impera”* was applied in order to solve all the problems.

But the military organizations were not the only ones to apply it. Civilian organizations, such as universities, did the same.

The universities were divided into departments centred around related disciplines.

By acting like this, the university's main activity, i.e. training students in various fields, was divided into coherent training stages that could be controlled by the technologies, knowledge, and personnel existing in the industrial age.

The principle was based on the brick wall idea. In order to build a strong wall, it was necessary for several entities (structures) to lay a brick at the right place and time. By combining all the parts, what resulted was a whole.

The principle worked well, except that not all bricks were identical, and those organizations that failed to join the parts efficiently, had disastrous results.

And military organisations did the same. The personnel were divided into different specializations (logistics, staff, human resources, security, etc.).

By combining the activities of all these groups, the commander obtained a more realistic image of the battlefield. The division of the battlefield into land, naval, air and spatial is also an example of division specific to the industrial age. By dividing it into small size components, it was possible to use an approach and to solve the problems with the help of the existing technologies.

Specialization – a deeper knowledge in all the fields of activity has resulted in an increase in the amount of information available in all fields. To manage a high amount of information by using the existing technologies, it was necessary for people to become specialized in fields that were increasingly narrow.

If we follow the example set by LEONARDO DA VINCI, whose wide interests ranged from art, and philosophy to mathematics, physics, engineering, etc., in the Industrial Age we have such personalities as ALBERT EINSTEIN whose breakthroughs in theoretical physics are world famous. This principle is applied within military organizations as well.Very narrow specialities allow for certain performances to be achieved, performances that whould have not been possible to achieve by someone with general knowledge in various fields. If we take as an example an air operation, we can see in order for such an operation to be carried out in optimum conditions, it is necessary to have structures ready to provide information about the systems dealing with: antiaircraft defense, detailed planning, air force units command, in-flight refueling, missions analysis, and search and rescue.

All these structures have highly specialized personnel, equipment, organization, and activities required to obtain maximum performances in every field.

Hierarchical organization – is the direct consequence of information transport lines becoming specialized in the Industrial Age.

To attain an organization’s objectives, it is necessary that all specialized structures be coordinated in such a manner that by combining the action of each structure, the final action of the organization is obtained.

It was as a result of this hierarchical organization that an intermediate management level has appeared, having the following functions:

- Understanding the organization’s objectives and rules;
- Sending the organization’s objectives and rules to subordinates;
- Drafting plans that allow for the integration with the organization’s objectives and values;
- Monitoring the subordinates’ performances taking corrective measures when necessary;
- Sending the feedback to the central management regarding the changes.

The hierarchical organization in the military structures is given by:

- 1 group = 6-8 soldiers; 1 platoon = 3-4 groups; 1 company = 3-4 platoons; 1 batallion = 3-4 companies; 1 brigade = 3-4 batallions;
- 1 division = 3-4 brigades; 1 army corps = 3-4 divisions; 1 army = 3-4 army corps.

Throughout the history, we can find the same structure within the military organization, including at a time when communications links were rudimentary.

In the Industrial Age, the communications systems developed significantly, but more in the direction of increasing the action range rather than the amount of information being sent, a fact which did not bring about a revolution in the organization of military structures.

In this type of organization, the information travel from the bottom of the hierarchy to its top and viceversa. The more the steps between the top of the pyramid and its base, the higher the time required for transmitting the information, as well as the margin of error. By controlling the information that travelled within the hierarchical structure, the elements of the military organization were also controlled. This happened because all the information (correspondence) addressed to a structure was addressed to the commandant of that structure, and subsequently, it was distributed within the structure.This way, the information was forced to travel withing the hierarchical structure and not directly between the initiator and the addressee of the information.

Optimization – the mark left by the industrial age on the military environment has led to a division of the battlefield, the setting up of specialized structures, and their hierarchical organization.

Using this approach, complex military operations were transformed into a set of simple and easy to control actions owing to the industrial age tools. This type of approach is liniar. The next step was optimizing these processes.

The second pillar of the industrial age (alongside the first one in which the whole is the sum of the parts) was that each part had the best solution. This type of approach is a result of the fact that officers' training was based on university programmes in the engineering field. The search of the optimum yields results when the threats are not numerous and an optimum answer can be found for each. For instance, during the Cold War, both the USA and the USSR created structures and plans in order to achieve victory. The moment a new type of threat appeared, the structures created for the Cold War could not handle the change, as it happened during the war in Afghanistan with the Russian army or during the Vietnam War with the American army. This kind of example can be frequently found in nature. The living organisms that specialized in a certain type of food disappeared the moment the weather conditions changed, and that kind of food no longer existed. Specialized organisms failed to adapt to the new conditions.

The ability to adapt to the new conditions is the key to survival.

Separation – given the fact that by combining all the parts, the whole is obtained, one of the most important activities in the Industrial Age was the separation of the action range of these parts in order to avoid an overlap.

These overlaps had to be avoided so that fratricide would not be fostered.

Some of the parts'separation measures are, as follows:

- Shooting sectors;
- Altitudes that were banned for own planes;
- The division of the routes among the logistics units;
- Rules of engagement specific to each theatre of operations.

By setting these separation limits among a military organization's components, commanders are provided with increased freedom of action inside that zone. This separation is a consequence of the lack of information and of accepting the fact that the whole is the sum of the parts.This concept is still valid when we deal with things, actions, linear actions, but under certain circumstances the whole is greater than the sum of parts, when the parts combine and act together.

Centralized planning – planning has become the main element in the industrial age because in order to obtain the whole, it was necessary for the parts to act based on a plan.

Military plans included the following elements:

- Mission - what had to be carried out and the each structure's contribution to mission accomplishment;

- Means available to carry out each component of the mission;
- Imposed limitations (responsibility areas of all units);
- Time planning of actions;
- Contingency plan for situations that may appear while the initial plan is being put into practice, others than those foreseen.

Decentralized execution – was characteristic of highly professional armies, such as the German army during WWII.

The commanders were aware that owing to the rapid developments on the battlefield and the fact that not situations could be foreseen, no plan was perfect.

The words of a great tactician, HELMUTH CARL BERNARD VON MOLTKE (1800-1891) are well known:

„No battle plan survives contact with the enemy”.

Given this fact, initiative and decenstralised execution were encouraged to accomplish the assigned mission.

Therefore, it can be seen that, taking into account all these elements, the military organization in the industrial age was using a simple, cyclic, OODA cycle-like command and control system.

This command and control mechanism is adaptive, its scope being to adjust its actions to changes produced.

This system yields good results in an environment in which threats are not multiple or varied, and the speed of events is low.

The Information Age does not affect only military organizations. It leaves its mark on the entire human society.

The decrease in the price of information has resulted in information being accessible to a larger number of people. This has also resulted in more diverse and numerous threats.

The 9/11 attacks showed that we had passed the age in which confrontations took place between two military blocks, which was characteristic of the cold war. Nowadays, threats are much more subtle, but they can generate more damaging effects.

Also, the information transmission speed brings about an increase in the speed of events. It can be deduced that military organizations based on the industrial age model cannot handle new challenges.

The natural question is:

How can a military organization able to face the new challenges be created?

Firstly, it should allow for the information to be transferred to all its components without any barriers artificially created by a hierarchical-like structure. This implies that the components of a military organization need to be interoperable.

Interoperability allows for the information to be transferred between the structures that form a military organization, and between a military organization and a civilian one. To achieve interoperability, apart from the organization-related measures, it is necessary to creat an informational infrastructure that would allow for all military and civilian structures to be connected in a network. Although it involves high costs, the informational infrastructure is easy to set up. What is more difficult is to change people's mentality, to educate a new generation of officers that would accept the distribution of information with the purpose of achieving an organization's common objectve.

The second element is adaptability. The military organization needs to be adaptable to the new types of threats, of which some cannot be foreseen. Interoperability and adaptability are the two fundamental characteristics of the military organization in the Information Age. Presently, there is no unanimously accepted organizational model. There are several directions of development for the military organizations, which would fit the requirements of the information age.

Although we cannot speak about an organizational model characteristic of the information age, a few elements are commonly accepted:

- To allow for an efficient distribution of a large amount of information at high speeds between the components of an organization, it is necessary that these components use powerful information systems connected in a network. In other words, a physical infrastructure is required to allow for the exchange of information. This infrastructure exists in the physical domain.
- Secondly, it is necessary that the information exist in order to become available to all the components of the organization. All these are to be found in the information domain.
- Thirdly, it is necessary that people using this information to change their approach from the concept "necessity to know" to the concept „ necessity to distribute". This change of attitude is in the cognitive domain and is accompanied by a series of new rules of human interaction.

If in the case of the first element, things were relatively simple, depending on the access to technology and the organization's financial power, in the case of the other two elements things are much more complex. In the case of the second element, the existence of information, a detailed analysis is made in the chapter dealing with the information warfare.

Briefly, information needs to be acquired on different channels and used, but at the same time, it has to be protected so that it is not used by the opponent.

When the premises of your victory are based upon the efficient use of information, its protection becomes the organization's main priority.

In the second case, the change in people's attitude should come from identifying new relations between people and, implicitly, between the structures making up an organization, and should continue with adapting the education system to the new requirements.

Although from all of the above mentioned one may think that the hierarchical model of organization is an obstacle in transmitting the information, this is not entirely true.

In fact, only the intermediate steps between the central command structure and the combat units are the ones that hinder information transfer.

Modern technology allows for a direct exchange of information between the two structures.

This implies that the intermediate structures should play only an administrative role in creating and maintain the combat units, while the actions should be directly led by the central structure in the case of an organization or another model in the case of a consortium.

This way, the part with the structure creation and maintenance, which requires more time in order to act, is disconnected from the part concerned with the use in action, which requires lower reaction time.

And since the missions that need to be carried out by the specialized structures cannot be foreseen every time, or because the speed of action is high, it is necessary to have flexibility when groups of structures are created to handle the missions.

To this end, it is necessary that all structures be interoperable and adaptable, and be ready to act in groups of structures that are newly created for a limited period of time for the specific missions to be carried out.

And by interoperable and adaptable structures I do not mean only structures belonging to military organizations.

Many times, in the information age, the structures belonging to both military and civilian organizations have been forced to work together in order to accomplish missions.

Naturally, it is necessary to have a network that would comprise all the structures of a society. However, it is necessary to have standards that would allow for the networks of each struncture to be interconnected when they work together.

To support the organizations that have started to get adapted to the requirements of the information age, NATO has devised a working instrument that would allow all to measure the development of progress. The instrument is called NATO NETWORK ENABLED CAPABILITY C2 MATURITY MODEL. [3]

The use of this instrument helps to determine to what extent a network of structures operates in accordance with the Informaion Age requirements.

To understand this instrument, several clarifications need to be made:

➢ Team – it consists of more people who share common interests and objectives. They train together and develop a common working culture. A team is made up of a leader and the members that fully understand the responsibilities, competences, and their limits in making decisions;

➢ Organization – consists of several teams centred around a common vision, common values, rules, laws and procedures, between which there is an open exchange of information and a certain degree of freedom in carrying out the mission and fulfilling the vision;

- Group of organizations – more organizations that cooperate in their interest or for a common interest. The links between them are not developed and they lack a central command authority, which implies the existence of certain self-synchronization level.

Given the fact that at the team and organization's level it can be implemented an organizational model that would allow for information to be efficiently distributed, and owing to the existence of a well defined leadership authority, NATO NEC C2 Maturity Model measures the degree to which the group of organizations is able to meet the requirements of the Information Age. Within the group of organizations there is no well defined leadership authority, there are no common rules and procedures, and the organizations making it up act together only under certain circumstances.

To establish the interaction level between the organizations within a group, three axes have been defined:

- Delegating the leadership authority to the group – it refers to the degree to which organizations hand over decision-related competences to the group to accomplish a common purpose;
- The information links between the group's organizations – refer to the possibility of interconnecting the information networks, and the interoperability between the organizations at the level of equipment and procedures;
- The information distribution between the member organizations - it refers to the level of information distribution necessary to fulfill the common objective by all the group's organizations.

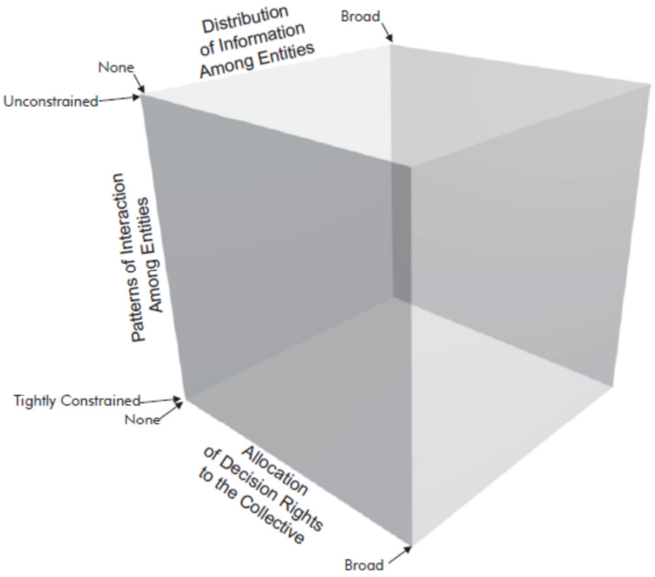

Distribution of Information Among Entities
None
Broad
Unconstrained
Patterns of Interaction Among Entities
Tightly Constrained
None
Allocation of Decision Rights to the Collective
Broad

Fig. 13 The axes of interaction between the organizations within a group [3]

By using these three axes that comprise all the three domains – physical, informational, and cognitive – without delimiting them strictly, the model uses five steps of evolution of the group of organizations, from the least favourable to the situation best adapted to the challenges of the Information Age. These steps are:

- Conflicted;
- De-Conflicted;
- Coordinated;
- Collaborative;
- Edge. [3]

1) **Conflicted** – at this level there is no interaction between the organizations of the group because there are no common objectives,

and thus each organization manages itself individually towards achieving their own goals. There are no connections that would allow for the exchange of information, and obviously, there is no exchange of information between the members of the group. These organizations act in isolation without being able to handle the entire range of threats spefic to the Information Age.

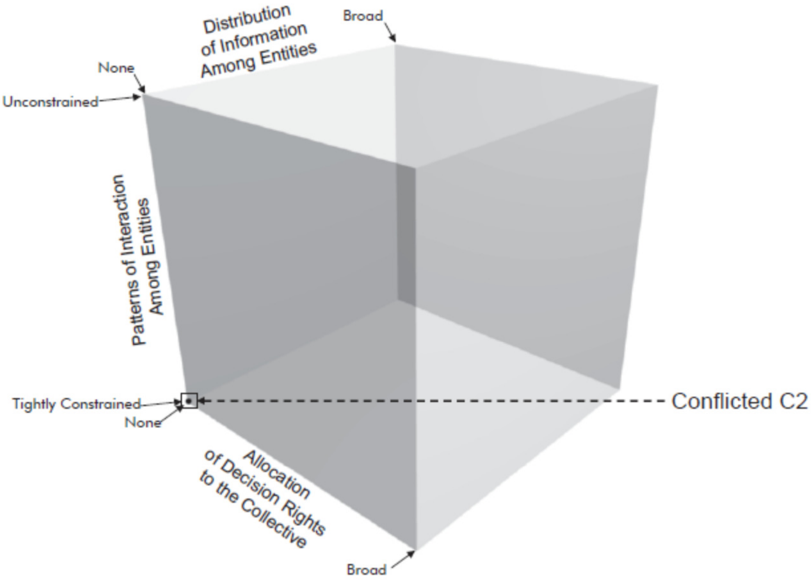

Distribution of Information Among Entities
Broad
None
Unconstrained
Patterns of Interaction Among Entities
Tightly Constrained
None
Conflicted C2
Allocation of Decision Rights to the Collective
Broad

Fig. 14 The isolated level of interaction between the organizations within a group [3]

2) **De-Conflicted** – at this level there is minimum collaboration between the organizations of the group, which help avoid overlap in terms of actions carried out by the members. The ranges of action for each organization are clearly delimited.

This implies that all the members of the group hand over part of the leadership authority to the group in order to set these limits.

Also, it is possible to interconnect the informational networks, while the information regarding the areas of responsibility is distributed to all the organizations of the group.

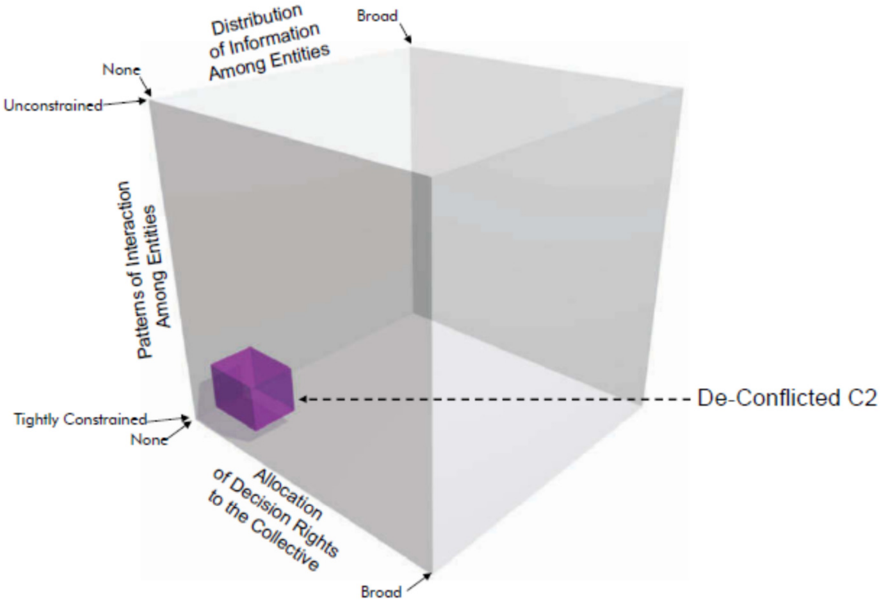

Distribution of Information Among Entities
Broad
None
Unconstrained
Patterns of Interaction Among Entities
De-Conflicted C2
Tightly Constrained
None
Allocation of Decision Rights to the Collective
Broad

Fig. 15 The separate level of interaction between the organizations within a group [3]

3) **Coordinated** – at this level, each organization’s command authority is partially delegated to the structure responsible with carrying out the mission in order to fulfill a common objective.

This implies the possibility for the information to be exchanged between the group’s organizations, and to be available to certain members of the group in charge of carrying out the mission.

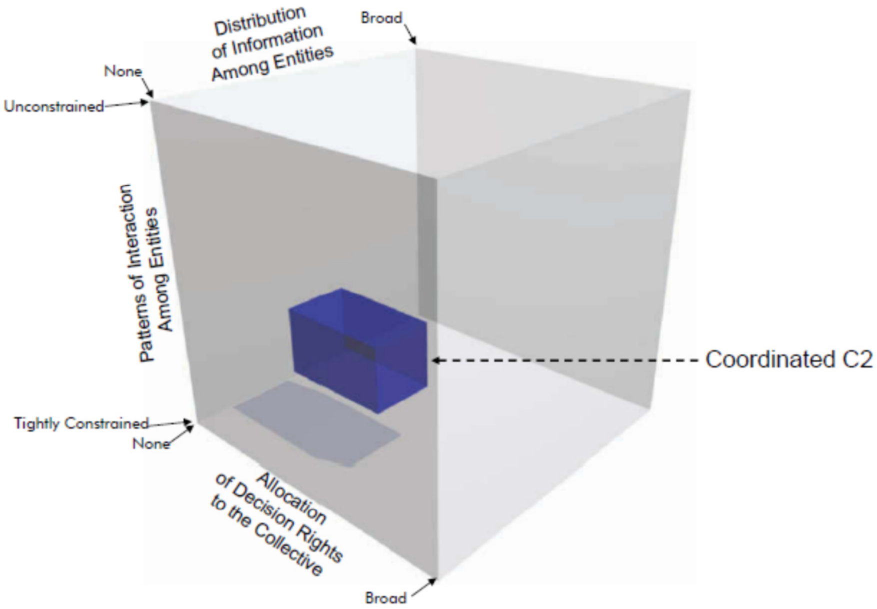

Distribution of Information Among Entities
Broad
None
Unconstrained
Patterns of Interaction Among Entities
Coordinated C2
Tightly Constrained
None
Allocation of Decision Rights to the Collective
Broad

Fig. 16 The coordinated level of interaction between the organizations within a group [3]

The level of interaction between the group's organizations is limited to the minimum required for mission accomplishment for which certain members need to coordinate their actions. Apart from these missions, there is no interaction.

4) **Collaborative** – at this level, the group's organizations have set and approved common objectives and a common action plan for the members. In this situation, the organizations, even if they have other objectives, they cannot conflict with the common objectives, and each organization's plans need to converge with the common plan.

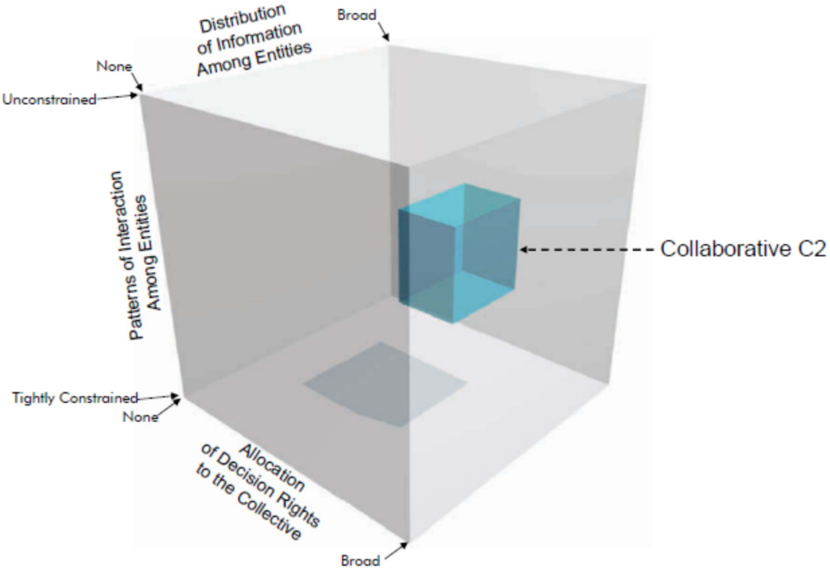

Distribution of Information Among Entities
Broad
None
Unconstrained
Patterns of Interaction Among Entities
Collaborative C2
Tightly Constrained
None
Allocation of Decision Rights to the Collective
Broad

Fig. 17 The collaborative level of interaction between the organizations within a group [3]

This implies that a great deal of the command authority has been handed over to the group and that there are strong connections between the organizations'digital networks, and that the information is distributed to all the members.

The group members collaborate in order to achieve the common objectives.

Nevertheless, there is strong exchange of information between the group members, and the synchronization of their actions is made with the help of an action plan.

This situation is specific to the most advanced command and control systems in the Industrial Age.

Given the fact that carrying out an action plan requires a certain period of time, this level of command and control will not be able the face the challenges given the high speed at which threats develop in the Information Age. It only takes one more step.

5) **Edge** – at this level, the organizations of the group do not need an action plan. They are able to self-synchronize. Self-synchronization is possible is there are strong connections between the information networks of all the organizations that would allow all members to have access to available information at a certain time.

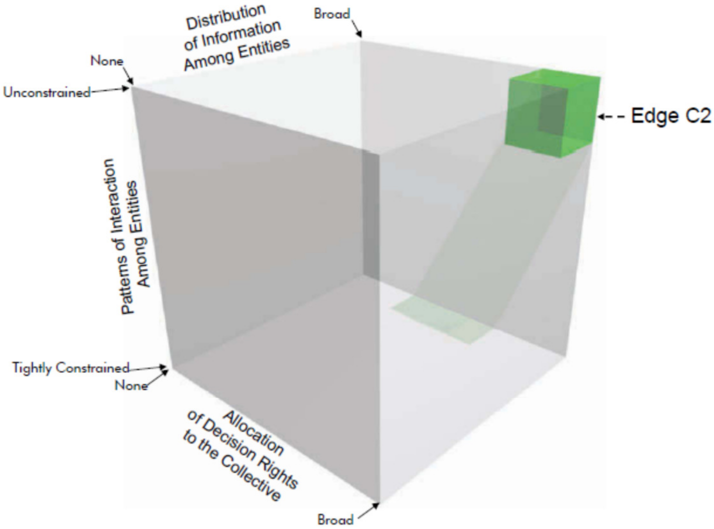

Distribution of Information Among Entities
Broad
None
Unconstrained
Edge C2
Patterns of Interaction Among Entities
Tightly Constrained
None
Allocation of Decision Rights to the Collective
Broad

Fig. 18 The ideal level of interaction between the organizations within a group [3]

The power to decide is decentralized and is handed over to those who have to act. Those who carry out actions have access only to available information, but they also have the authority to make decisions at a certain time, which increases the group's capability to respond.

At this level, apart from self-synchronizing their actions, the organizations of the group are not capable of organizing themselves in structures adapted to the threats.

This way, the requirements of the Information Age in terms of interoperability and adaptability to foreseeable or unforeseeable threats are met. The structure of the group is flexible, and its power resides in the capability to distribute the information to the group members, rather than in the information control.

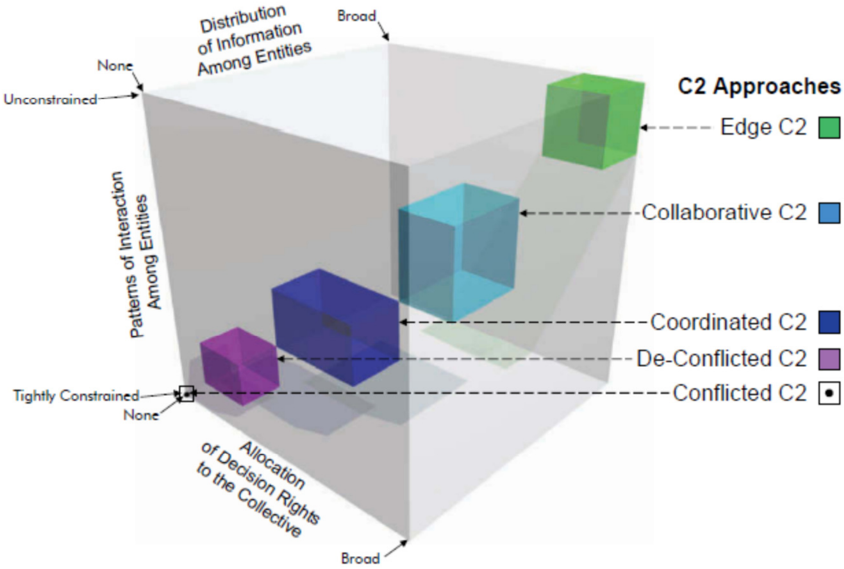


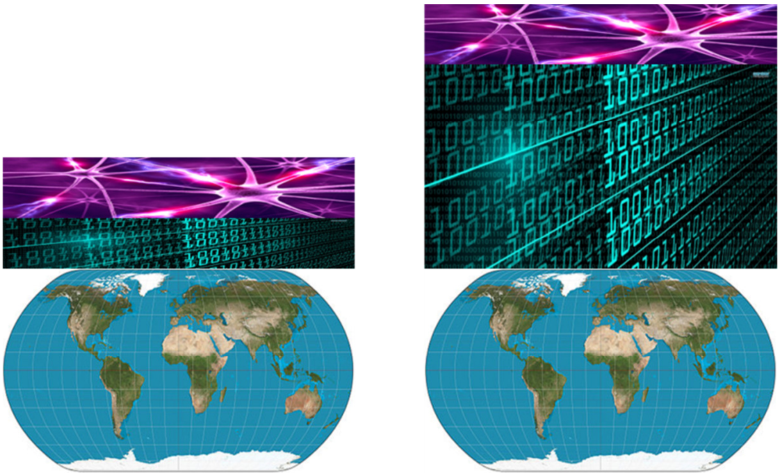
Fig. 18 The levels of interaction between the organizations within a group [3]

The transition from the concept „necessity to know" to the concept „necessity to distribute" is made.If the power of the group resides in its capability to distribute the information to all its members, it is necessary that all this information be gathered and, expecially, that the distribution networks be protected. Thus, a new concept of war appears the Information warfare.

2 INFORMATION WARFARE

2.1 The Concept of Information Warfare

The effective use of information, in order to obtain a decisive advantage against opponents has its roots buried deep in human history.



a) Industrial Age b) Information Age

Fig. 19 Information domain development

If radical measures have been taken to amend the information flows, that were synthesized by the network centric warfare, in order to make the needed information available to members of the military organization in due time, it is necessary that this information structure to be fed with the required information.

If, in the past, war`s gravity center was found in physical domain, which influenced the information and cognitive domains, during the information age the gravity core migrated to the information domain that further on influenced the cognitive and physical domains.

As we noticed in the case of network centric warfare concept and information warfare there isn`t a universal accepted definition or a common theory. Anyway, there are some common aspects found in the approaches regarding the information warfare.

Thus, information warfare is defined as the totality of actions taken to gain information superiority through influencing, to a higher or lower extent, the counterparts`information, information processes, systems and computers networks together with protecting personal information, information processes, systems and computers networks. Starting from this definition, we can determine the basic components of information warfare.

a) Information research – comprises the totality of information acquisition techniques regarding the enemy, own forces and fighting area, processing, distribution, analysis and information update;
b) Information attack – represents the totality of the adversary`s disinformation measures;
c) Information protection – consists in all measures taken to stop information gathering about own forces by foes and the minimization of effects caused by disinformation actions driven by the enemy.

Given that the information war is not limited to military intelligence, the information conflict space includes the following specific forms:

a) Command and Control Warfare (C2W) – operates in military intelligence and is designed to destroy the enemy's command and control structure;
b) Information Based Warfare (IBW) – includes those actions of creation, protection and neutralization of entities dealing with

obtaining information in real time; it contains SIGINT as well – SIGnals INTelligence – which refers to a type of research derived from interception and analysis of external traffic data and of internal content of space electromagnetic signals, and of computers network signals;

c) Hacker Warfare „software pirates" (HW) – acts on the foe's computer networks using specialized programs;

d) Economic Information Warfare (EIW) – seeks to ensure those information which provide an economic advantage;

e) Cybernetic Warfare (CybW) – constitutes all actions taken in virtual reality space in order to cause enemy loss in physical field.

In terms of time to conduct these types of information war, these occur in all three phases of confrontation: peace, crisis and conflict. Since this analysis focuses on military organizations, we shall further on analyze the command and control warfare.

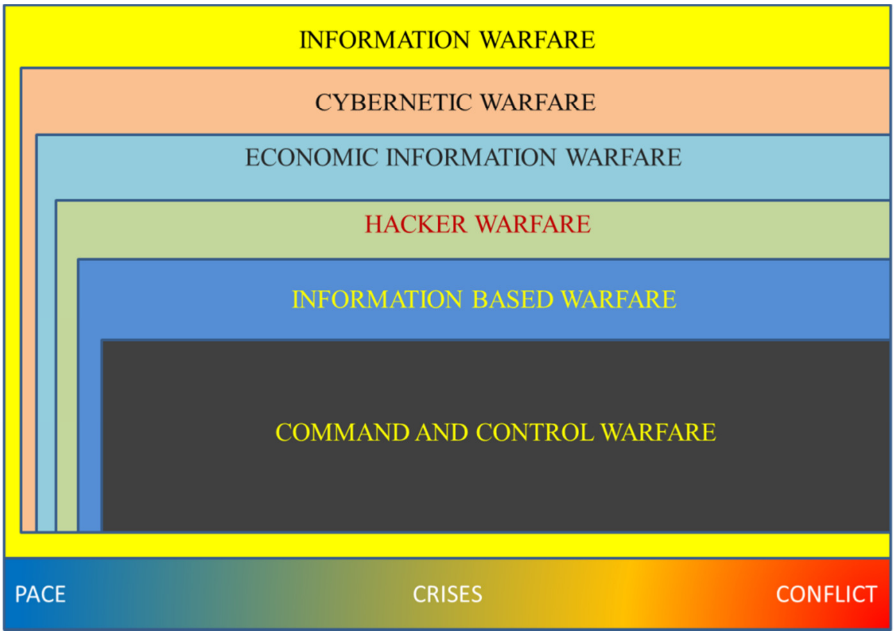

INFORMATION WARFARE
CYBERNETIC WARFARE
ECONOMIC INFORMATION WARFARE
HACKER WARFARE
INFORMATION BASED WARFARE
COMMAND AND CONTROL WARFARE
PACE
CRISES
CONFLICT

Fig. 20 Information Warfare Components

2.2 Command and Control Warfare

Command and Control Warfare represents that part of information war applied in military operations. Command and Control Warfare uses joint Psychological Operations (PSYOP), Military Deception (MILDEC), Security Operations (OPSEC), Electronic Warfare (EW) and physical destruction, based on information obtained through intelligence structures to protect own information or to influence, reduce or destroy the enemy's control system control while protecting the own command and control system against enemy actions.

This approach makes the transition from resource use to destroy the enemy`s shooting systems, to the use of resources for ultimate destruction of the enemy`s command and control system.

It is more effective to fight with disorganized units and it is much less expensive to hit your foe`s command and control system.

Since the victory premises are in the information domain and consist of the ability to spread information within their own system, it is obvious that the main action should focus towards the enemy`s command and control system.

If influencing it in the desired direction and reducing information flow so as OODA cycle speed to fall are gained, the confrontation between well-managed striking systems and the disorganized ones have only one result that is, defeating those with lower command and control system. And finally, the price paid for this result is much lower (victims, consumed material and financial resources).

This approach allows a certain degree of war efficiency. Elements of command and control warfare:

- Psychological Operations (PSYOP) – represents all actions taken to emotionally influence the enemy at political, military, economical and information level to support own operations;
- Security Operations (OPSEC) – represents all actions taken to prevent the enemy to obtain the information necessary for an accurate estimation of the operational situation;
- Military Deception (MILDEC) – represents all actions undertaken to determine the enemy to estimate incorrectly the operational status so as to expose to vulnerabilities and engagement of new forces in our desired direction;
- Electronic Warfare (EW) – includes all actions undertaken for the private use of the electromagnetic spectrum;
- Physical Destruction – represents all actions taken to control the destruction of enemy command and control systems in order to achieve the objectives of command and control war.

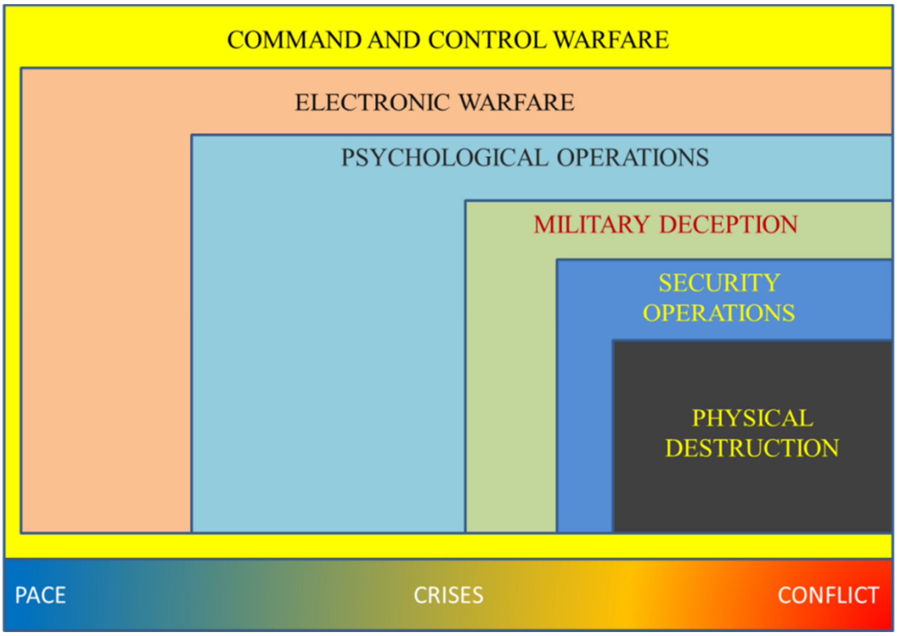


Fig. 21 Command and Control Warfare Components

Within the information war, it is necessary to provide with information obtained through other channels so as to effectively integrate all these elements of command and control war. From this point of view, the command and control war represents the combat element which implements information and orders from a higher level.

Once again it turns out that the flow of information plays a decisive role in achieving victory, and that a direct consequence of the existence of a strong information flow is represented by the integrated action of several organizational structures in order to achieve a common goal. The integrated action on more levels leads to more effective exploitation of enemy`s vulnerabilities with minimal costs.

2.2.1 Psychological Operations

Psychological Operations (PSYOP) – consist in sending that information to the adversary in order to influence its emotions, motivations, objectives, and last, but not least its behavior at the individual, group, organization or government level.

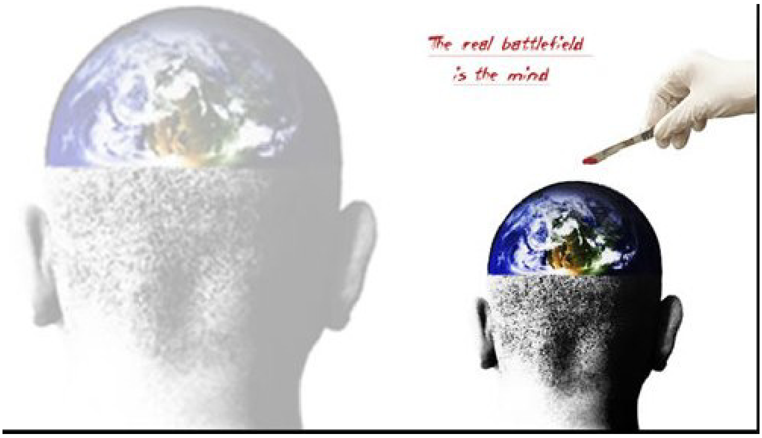


Fig. 22 Psychological Operations (PSYOP)

PSYOP takes place in all three phases of military confrontation, that is, peace, crisis and conflict in order to inform and influence the opponent.

PSYOP can save lives both among its forces and among enemy ones, reducing the enemy`s fighting desire. By reducing the morale related to the ability to act effectively, PSYOP discourages aggressive actions, creates opposition among opponents that can ultimately lead to surrender without a fight.

PSYOP missions are as follows:

- Commander counseling during combat actions planning in order to maximize the effects and to reduce side effects among non-combatant population;
- Influencing the enemy`s non-combatant population by sending those pieces of information and encouraging those behaviors to support military operations;
- Sending information to the enemy`s non-combatant population to support humanitarian efforts to reduce the suffering of those affected by military operations and last, but not least, to ensure order among the civilian population;
- Creating those communications channels so as the commander can convey messages to the enemy`s civilian population;
- Counteracting the enemy's actions of propaganda, disinformation by presenting own actions in a favorable light and preventing the creation of a civilian opposition against their troops.

Starting with 2010 the United States used for psychological operations the term military information support operations. In essance missions are the same but the name does not cause a negative reaction among the civilian population.

According to the purpose there are two types of psychological operations:

- Cohesive;
- Divisive.

Psychological operations that aim at achieving cohesion between own troops and civilian population or enemy troops focus on the following aspects:

- Strengthening national unity;
- Promoting a favorable image of the government;
- Providing the target audience with information;
- Improving civil-military cooperation;
- Counteracting hostile propaganda;
- Public unification against a common enemy;
- Shifting public attention from the mission's unfavorable issues.

Psychological operations aimed at dividing the enemy`s forces so as to reduce the ability to take action, have the following courses of action:

- Exploiting the adversary's vulnerabilities and mistakes;
- Encouraging dissentions among opponents;
- Weakening opposition's power towars its own troops;
- Intolerances exploitation;
- Encouraging desertions and lack of action;
- Encouraging self-interest at the expense of group interest.

2.2.2 Military Deception

Military Deception (MILDEC) – comprises those actions to mislead the enemy's intelligence structures regarding their own possibilities, intentions and operations carried out by own forces.

These actions are performed by transmitting information, images or false statements that will cause the opponent to take those actions that facilitate own troops to accomplish their objectives.

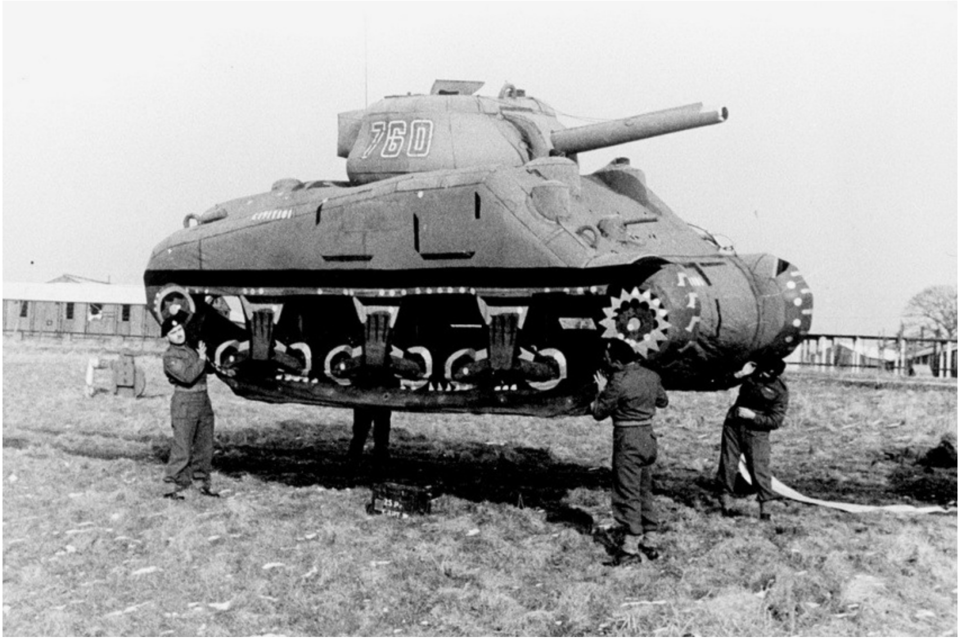


Fig. 23 Military Deception (MILDEC)

Military deception operations are part of the military operations plan and are carried out to determine the opponent to wrongly engage forces in combat, so as to make it uncover its weaknesses and strengths, to expose its position and future intentions. Furthermore, military deception operations can be aimed at excessive loading of the enemy`s analysis and information processing capacity that causes him to use secondary data processing systems with lower characteristics that can be easily exploited by own forces.

Military deception is achieved through degradation of opponent's opportunities to acquire information through sensors and by manipulating information transmitted by them.

In conclusion, military deception seeks to create the enemy a misleading picture of the battlefield to get it take predictable actions that can be successfully exploited by own forces so as to achieve victory.

2.2.3 Operations Security

Operations Security (OPSEC) – is the process through which information is identified and protected, even though unclassified, they can create an advantage if used by foes.

The steps of this process are:

- Identification of critical information;
- Determination of potential threats;
- The analysis of own vulnerabilities;
- Risk assessment;
- Implementation of appropriate measures for each situation.

The steps of this process take place in real time so as to:

- Identify those information that can be gathered by enemy's research systems;
- Determine how this information can be used by our enemy against us;
- To implement those measures to minimize vulnerabilities and risks of exploitation of that information by the enemy.

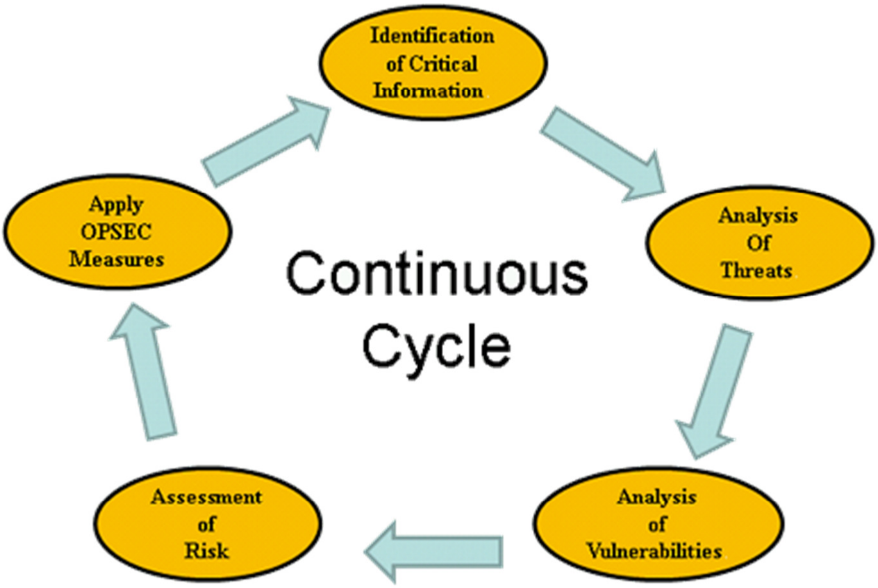


Fig. 24 Operations Security (OPSEC)

Unlike traditional forms of security operating with classified information at different levels, depending on their importance, information subject to security operations are classified and can easily get into the hands of the enemy.

Securities operations are closely linked to military operations carried out by own troops and propose measures adapted to these missions only during their length. This causes great flexibility in implementing this process with measures that may be unique, due to the type of military operations and their development conditions.

2.2.4 Physical Destruction

Physical Destruction – refers to the destruction of information processing systems within the enemy's command and control structure. Physical destruction is applied to sensors network, to critical nodes from the structure of C2 communication systems, computer networks or command centers.

This method involves the use of fire systems.

Fig. 25 Physical Destruction

The process of hitting targets may be divided into three stages: targets acquisition, hitting targets and evaluating the effects.

Given that the enemy can restore its combat capability after such an attack, it is necessary that physical destruction actions to be synchronized with the other actions of the military operation, so as to maximize results.

Since, it is costly and inefficient to destroy the whole enemy’s command and control system, physical destruction actions aime at obtaining an advantage of the moment to be exploited effectively. Through these hits, the enemy’s command and control system is destabilized leading to slowing the enemy’s OODA cycle, allowing their own troops to act within the enemy’s OODA cycle.

Physical destruction is specific to the armed forces and it is carried out during the conflict confrontation period.

2.2.5 Electronic Warfare

Electronic Warfare (EW) – is defined as the operating military action involving the exploitation of the electromagnetic spectrum which presuposes the emission interception and identification, electromagnetic energy engagement, including the directed energy, while reducing or preventing hostile actions within the electromagnetic spectrum. [4]

Electronic warfare actions aim at the employment of electromagnetic spectrum for its own use while limiting its use by the enemy.

In this context, any device involving the use of electromagnetic energy is important in terms of electronic warfare.

In the information era, military relies heavily on the use of the electromagnetic spectrum for communications, electronics, surveillance, research, navigation, weapons systems, own protection, etc.

It becomes obvious that the dominance of the electromagnetic spectrum is a crucial component of military operations in the information age, based on intensive use of information systems and electronic communication in general.

In order to dominate the electromagnetic spectrum both offensive action (electronic attack EA) and defensive actions (electronic defense ED) are needed.

These two actions always require informational support provided by electronic surveillance actions (ES).

Electronic warfare is an important form of strategic, operational and tactical insurance which is organized and implemented in all forms of combat actions in all types of armed forces.

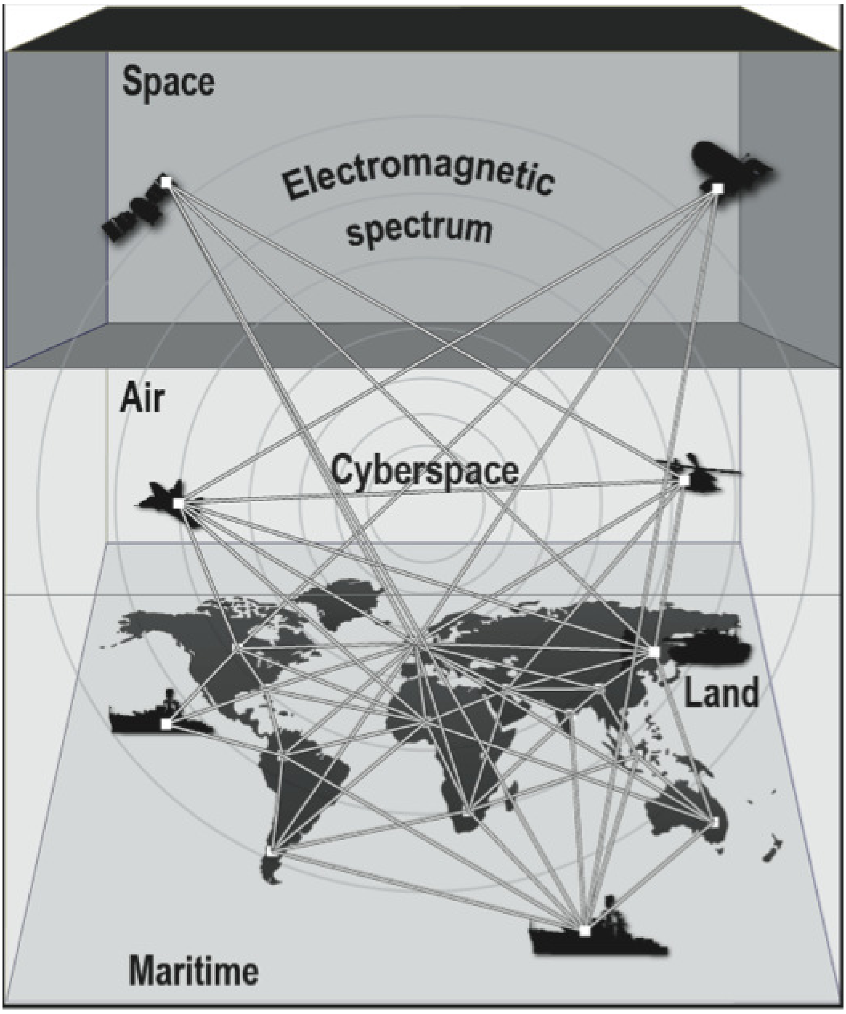


Fig. 26 Electronic Warfare (EW)

Considering this, it is necessary that electronic warfare actions to be synchronized in all types of armed forces to the efficient exploitation of the electromagnetic spectrum itself.

3 ELECTRONIC WARFARE

Electronic warfare is the miltary action within the electromagnetic spectrum to exploit in its own interest.

To achieve this objective the following specific actions are required:

- Electronic Support Actions (ES) carried out to ensure the information necessary to conduct other actions of electronic warfare;
- Electronic Attack Actions (EA) conducted to eliminate, neutralize or reduce enemy's threats electromagnetic spectrum;
- Electronic Defense Actions (ED) conducted to reject the enemy's electronic attack.

3.1 Electronic Spectrum

As results from the definition of electronic warfare, the electromagnetic spectrum is the environment in which it takes place.

It is noticed that to the three environments in which military operations are conducted (sea, land and airspace) a new environment is added, the electromagnetic one. Before analyzing electronic warfare it is necessary to understand what the electromagnetic spectrum really is.

To understand the electromagnetic spectrum it is necessary to go back to the origin of its discovery by JAMES CLERK MAXWELL (1831-1879), the theoretical and practical demonstration which was made in 1886-1887 by HEINRICH HERTZ RUDOLF (1857 -1894).

In 1865, JAMES CLERK MAXWELL manages to combine the electric field theory with the theory of the magnetic field, creating their electromagnetic field, which in theory proves the existence of electromagnetic waves and that they travel at the speed of light ($c=3x10^8$ m/s).

Electromagnetic field theory is included in four equations known as Maxwell's equations:

$$\nabla \cdot D = \rho_V \qquad \nabla \cdot E = \frac{1}{\varepsilon_0}\rho \tag{1}$$

$$\nabla \cdot B = 0 \tag{2}$$

$$\nabla \times E = -\frac{\partial B}{\partial t} \tag{3}$$

$$\nabla \times H = \frac{\partial D}{\partial t} + J \tag{4}$$

Viewed as such, these equations do not seem to explain the existence of electromagnetic waves.

I will present below each equation in part to understand the contribution of each to the electromagnetic field theory.

The first equation is also known as Gauss's law and it describes the behavior of the electric field around electric charges.

The sign is called the nabla operator and it represents the divergence. The divergence is an operator that measures how much a vector field exits / enters a point. The divergence of a vector field is a scalar.

To understand what phenomenon describes the divergence operator is required to imagine the vector field as a watercourse. If the divergence is a positive number it means that water flows outward from that point like a spring. If the divergence is negative, then the water flows from the outside into that point, as a leak.

Given this, we can say that Gauss's law in this form describes the behavior of the electric field at a point, or, that in any point in space, the electric field occurs in accordance with this equation.

Considering that:

$$D = \varepsilon \cdot E \tag{5}$$

where:

D is electric induction [C/m^2];
E is electric field intensity [V/m];
ε is the electric permittivity of the environment in which the electric field is measured [F/m].

We may say that D does not depend on material and that it is a vector field which means that, at any point in space, it is characterized by size, guidelines and direction.

In the right terms of the equation, the symbol ρ_V represents the charge density within a given volume, whose unit of measurement is [C/m^3].

Now that we have identified all terms of the equation, we can say that, if within a point in space there is an electrical load ($\rho_V \neq 0$) then the divergence (∇) of electric induction (D) in that point is zero. If in a point in space there is no electrical load ($\rho_V = 0$), then the divergence (∇) of electric induction (D) in that point is zero.

To understand how the divergence of electric induction varies, it is necessary to consider the equation in integral form. Let's consider an arbitrary volume V that is bordered by a surface S. We may say that V is a sphere and S represents the V sphere surface.

GAUSS's law in integral form becomes:

$$\int_V (\nabla \cdot D) dV = \int_V \rho_V dV \tag{6}$$

And for S surface:

$$\int_S D \cdot dS = Q \tag{7}$$

From equation 7 results that the total electric charge inside the V sphere (= Q) is equal to the size of the electric induction (D) that goes through the surface of the sphere (S). In other words, to determine the amount of electric flux that intersects the surface S it is required to determine the amount of electrical charge which is within the volume V.

The interpretation of equation 7 is the following:

The term $D \cdot dS$ refers only to the component perpendicular to the S surface. This component may be oriented towards the inside or the outside of the V volume. The term $\int_S D \cdot dS$ represents the sum of the vectors D*d*S from each point of S surface.

We can say that, according to Gauss's law, if withinan arbitrary V volume we have a positive charge, then, the electric induction vector sum ($\int_S D \cdot dS$) is equal to the size of the charge and their direction is towards the external volume.

If, inside an arbitrary V volume we do not have electric charge, then we have no electrical induction as well.

If inside an arbitrary V volume we have a negative charge, then, the sum of electrical induction vectors ($\int_S D \cdot dS$) is equal to the size of the charge and their direction is towards the inside volume.

Considering that forces are exerted among electric charges, then, we may write that:

$$F = \frac{q_1 q_2}{4\pi\varepsilon_0 r^2} \tag{8}$$

$$|E| = \frac{q}{4\pi\varepsilon_0 r^2} \tag{9}$$

$$|D| = \frac{q}{4\pi R^2} \tag{10}$$

The result is that opposite charges attract one another and similar charges reject themselves.

In conclusion, Gauss's law tells us that:

- The direction of the electric field lines is from the positive charges towards the outside and from the outside towards the negative charges;
- Electric field lines start from the electric charge surface and return to it;
- Electrical charges of the same sign reject eachother and opposite ones attract themselves;
- The divergence size (∇) of electric field induction (D) of any arbitrarily chosen volume (V) is equal to the amount of electric charge inside the volume (ρ_V).

GAUSS’s law for magnetic field

$$\nabla \cdot B = 0 \tag{11}$$

This equation tells us that the size of magnetic induction divergence (B) is zero.

According to this it results that:

- There are no magnetic monopoles;
- The magnetic induction divergence (B) is always zero for any arbitrarily chosen volume;
- The magnetic field lines form a closed circuit.

Faraday’s law

$$\nabla \times E = -\frac{\partial B}{\partial t} \tag{12}$$

Studying the behavior of electric and magnetic fields, Faraday observed that a changing magnetic flux produces an electromotive force or voltage.

$$FEM = -\frac{d\emptyset}{dt} \tag{13}$$

This equation states that the voltage induced in the electric circuit is opposite to the speed of change of the magnetic flux. This equation is also known as LENTZ’s law because he corrected Faraday's equation by adding the sign "-".

From the definition of the magnetic flux it results that:

$$\emptyset(t) = \int_S B(t) \cdot dS \tag{14}$$

The magnetic flux is the sum of magnetic induction on the surface arbitrarily chosen.

To find the total value of the electromotive force induced in circuit, induced electromotive forces gather in each point along the length of the electrical circuit.

$$FEM_{totală} = \oint d(FEM) \tag{15}$$

Considering that:

$$V = \int E \cdot dL \tag{16}$$

The tension between two points of a circuit is the sum of the electric field intensity along the length of the circuit.

$$E = \frac{dV}{dL} \tag{17}$$

Electric field intensity is a measure of the rate of change of electric power on the length of the circuit.

$$FEM_{totală} = \oint_{circuit} E \cdot dL \tag{18}$$

When reaching this point it is necessary to call on KELVIN-STOKES theorem showing that the integration of a vector field on a surface frame is equivalent to integrating the field rotor on that particular surface.

When calculating vectors, the rotor is an operator which highlights the rotation of a vector field, i.e., the axis of rotation and the rotation amplitude.

$$\oint_{circuit} E \cdot dL = \int_S \nabla \times E \cdot dS \tag{19}$$

$$\int_S \nabla \times E \cdot dS = -\frac{d}{dt}\int_S B(t) \cdot dS = \int_S \frac{-dB(t)}{dt} \cdot dS \tag{20}$$

$$\nabla \times E = -\frac{\partial B}{\partial t} \tag{21}$$

From equation 20 resulted that, if we have equality of two integrals on a surface and the surface can be chosen arbitrarily, then the quantities we integrate must also be equal.

In conclusion, the interpretation of Faraday's law is that:

- The electric current generates a magnetic field and a magnetic field generates an electric current;
- A variable magnetic field generates an electric field varying in space;
- An alternating electric field in space creates a variable magnetic field in time.

Studying Maxwell's equations, published in 1865, HEINRICH RUDOLF HERTZ (1857-1894) found that they are correct.

The existence of electromagnetic waves has been demonstrated by a series of experiments carried out during the years 1886-1887.

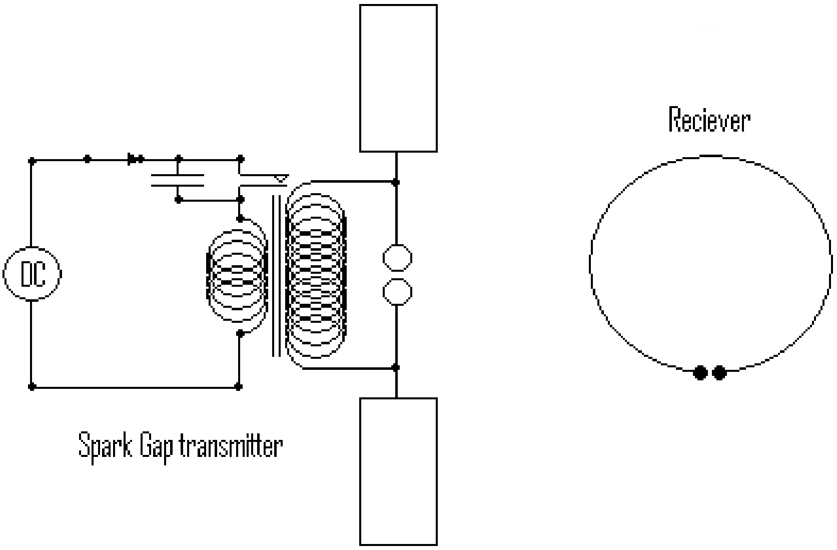


Fig. 27 Scheme of the experiment conducted by Hertz [5]

But HERTZ did not stop there, he managed to produce, transmit and receive the electromagnetic waves, to measure their speed confirming Maxwell's calculations, namely, that speed is equal to the speed of light.

During experiments, Hertz established that both the light and electromagnetic waves are described by Maxwell's equations.

Given that, he demonstrated the existence of electromagnetic waves, but also that they can be manipulated, created, transmitted and received, the unit of frequency is Hertz (Hz).

The electromagnetic spectrum represents all electromagnetic radiation in the universe.

To work more easily with the electromagnetic spectrum, it is arbitrarily divided into several regions, such as:

Radio spectrum – includes electromagnetic waves with a frequency $f \leq 3\times10^9$Hz or with the wavelength $\lambda \geq 10$ cm;

Microwaves – include electromagnetic waves with a frequency $3\times10^9 \leq f \leq 3\times10^{12}$ Hz or with the wavelength 10 cm $\geq \lambda \geq$ 0,01 cm;

Infrared waves – include electromagnetic waves with a frequency $3\times10^{12} \leq f \leq 4{,}3\times10^{14}$ Hz or with the wavelength 0,01 cm $\geq \lambda \geq 7\times10^{-5}$ cm;

Visible spectrum – includes electromagnetic waves with a frequency $4{,}3\times10^{14} \leq f \leq 7{,}5\times10^{14}$ Hz or with the wavelength 7×10^{-5} cm $\geq \lambda \geq 4\times10^{-5}$ cm;

Ultraviolet spectrum – includes electromagnetic waves with a frequency $7{,}5\times10^{14} \leq f \leq 3\times10^{17}$ Hz or with the wavelength 4×10^{-5} cm $\geq \lambda \geq 10^{-7}$ cm;

X-ray – include lectromagnetic waves with a frequency $3\times10^{17} \leq f \leq 3\times10^{19}$ Hz or with the wavelength 10^{-7} cm $\geq \lambda \geq 10^{-9}$ cm;

Gamma ray - include electromagnetic waves with a frequency $f \geq 3\times10^{19}$ Hz or with the wavelength $\lambda \leq 10^{-9}$ cm.

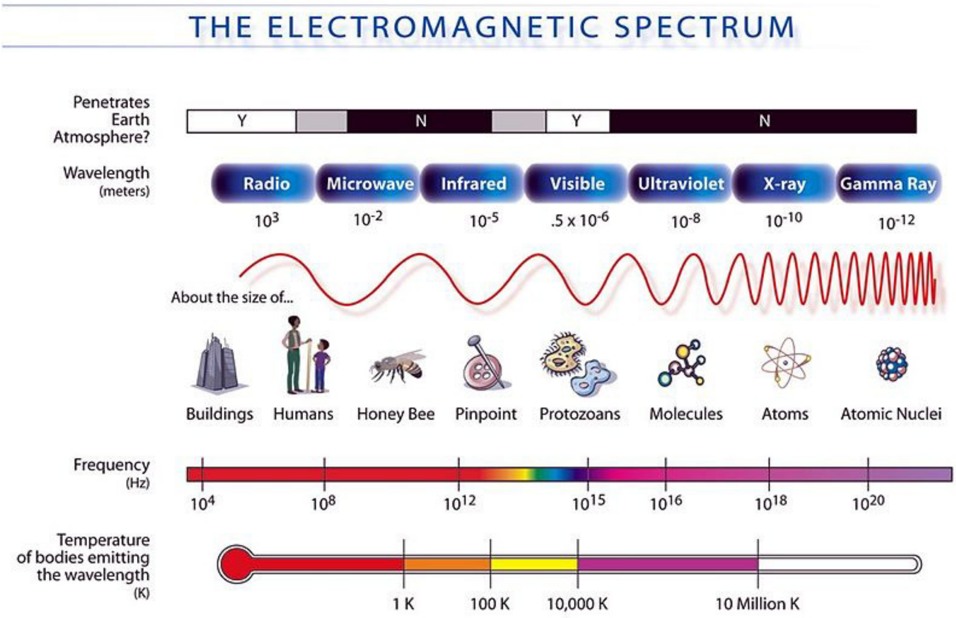


Fig. 28 Electromagnetic spectrum

The relation between frequency and wavelength is:

$$f = \frac{c}{\lambda} \text{ or } \lambda = \frac{c}{f} \tag{22}$$

$$\lambda_{metru} = \frac{3 \cdot 10^8}{f_{Hz}} = \frac{0{,}3}{f_{GHz}} \tag{23}$$

To learn the wavelength in centimeters we use the relation:

$$\lambda_{cm} = \frac{30}{f_{GHz}} \tag{24}$$

Exemple: for a frequency f=10GHz it results:

$$\lambda_{cm} = \frac{30}{10} = 3\ cm \tag{25}$$

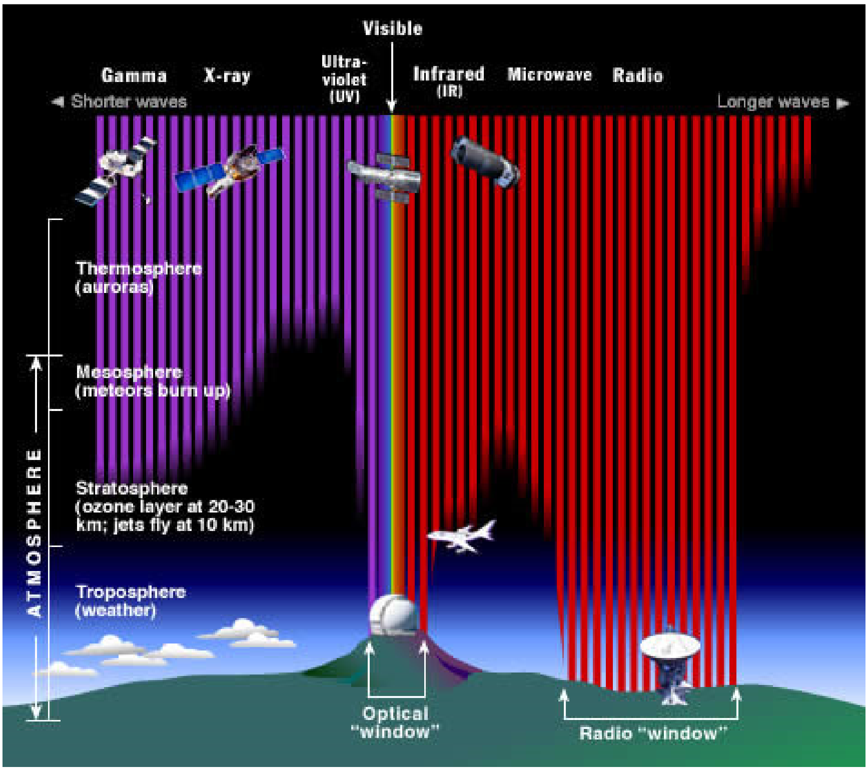


Fig. 29 Attenuation of electromagnetic waves in atmosphere

To get a clearcut picture of how the earth's atmosphere attenuates the electromagnetic waves, according to their frequency, it is necessary to analyze Fig. 29.

It is noted that most of electromagnetic waves from outer space, do not reach the earth because they are attenuated by the earth's atmosphere. However, there are two "windows" which provide the minimum attenuation of electromagnetic waves, for radio waves, and a part of the visible and ultraviolet spectrum.

According to the standards, the radio and microwave spectrum is divided into several frequency bands according to Fig. 30.

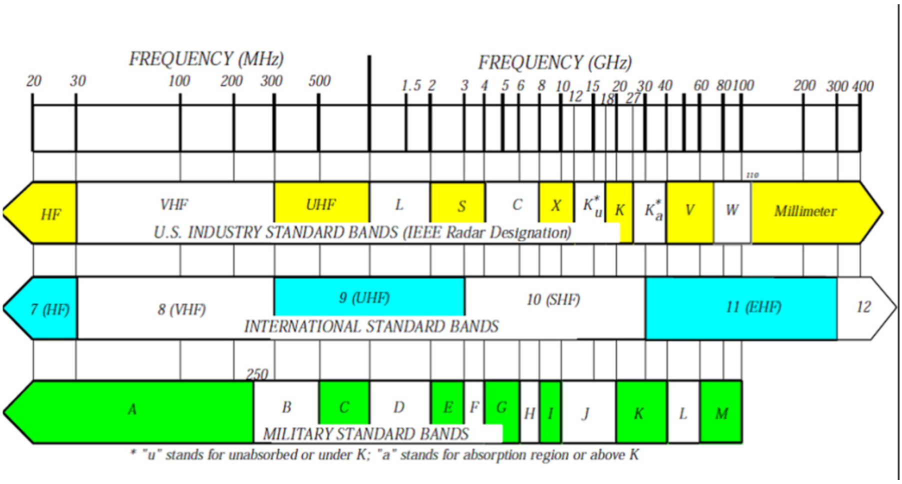


Fig. 30 Frequency bands according to standards

Considering that a lot of systems using electromagnetic waves have been developed in recent years and taking into account that the electromagnetic spectrum is a scarce resource, it is necessary to have rules of the electromagnetic spectrum management, both nationally and internationally.

From this point of view, all countries are sovereign in their own strategy of using the electromagnetic spectrum. Although this sovereignty ensures efficient exploitation and cooperation in fields like trade, transport, communications and mutual protection against interference, the states have signed the International Telecommunication Convention. This convention is the main instrument through which the International Telecommunication Union provides efficient use, in economic terms, of the electromagnetic spectrum internationally. The International Telecommunication Union (ITU) is the United Nations specialized body, based in Geneva, in which governments and the private sector coordinate global performed services for telecommunications networks. ITU Development Sector reflects technological progress and the specificity of the sector.

ITU differs from other UN specialized agencies through the private sector role reserved. In addition to Member States and Observers, ITU admits Sector Members and Associate Members as well, who are operators, research laboratories, equipment manufacturers, and other similar organizations.

The partnership with the private sector allows financial balance, the representation of all stakeholders, the contribution of technical expertise, etc.

ITU is composed of 191 Member States and 567 Sector Members. The union is divided into three sectors:

- Telecommunication Standardization (ITU-T);
- Radiocommunications(ITU-R);
- Telecommunication Development (ITU-D).

Fig. 31 International Telecommunication Union

The International Telecommunication Union Council, elected by the World Conference of Plenipotentiaries every four years, leads the organization, having as tasks the ITU setting policy and coordination of ongoing programs and financial resource management.

The quality of Member state in the ITU Council offers the opportunity to directly contribute to the decisions, regulations and rules created or to be created, with the initiative, amendment or repeal of provisions contained in the Acts of the Union.

Main activities:

- ITU is the leading organization for standardization in telecommunications. The standards developed by the ITU (known as referrals) cover practically all aspects of telecommunications;
- The cooperation with other standardization organizations, global or regional, has allowed to reduce incompatibilities and to speed-up the introduction of new technologies;
- ITU is an appropriate forum for discussing the new orientations of the sector and for promoting new business and technological models. These debates can take place both in meetings and conferences, as well as within the Forum of telecommunications policy, the global Seminar for regulatory experts or in other meetings held regularly;
- Performs allocation of radio refquency spectrum bands, the distribution of radio frequencies and registration of radio frequency allocations for space services, of any associated orbital position reporting satellite orbit or of any associated characteristics of satellites in other orbits, in order to avoid harmful interference of the radio stations and various countries. The management of these resources, along with the interconnection and interoperability, is, in fact, the original purpose for which ITU was created;

- Recognizing the crucial role of human resources, ITU promotes the transfer of skills through courses and seminars; it grants scholarships, finances the development of educational materials and provides experts and consultants to support the realization of projects in developing countries;
- TELECOM events (exhibitions and forums dedicated to technological innovations in telecommunications, organized by ITU) serve as a venue for representatives of governments and industry, allowing the detection of trends and facilitating contracts;
- Also, ITU Secretary-General serves as depositary of treaties related to telecommunications such as regional broadcasting agreements from Stockholm 1961, Geneva 1975, Geneva 1984, Rio de Janeiro in 1985, Geneva 2006, the Memorandum of Agreement on GMPCS (Global Mobile Communications Personal through Satellite), etc. and keeps the evidence of international satellite telecommunications, as well as the mobile satellite;
- Promotes and provides technical assistance to developing countries in telecommunications, promotes mobilization of material, human and financial resources of their implementation and access to information;
- Promotes and develops technical facilities and most effective promptness on improving the efficiency of telecommunication services, increasing their usefulness and making them available to the general public as much as possible;
- Promotes, internationally, the adoption of a comprehensive approach to telecommunications issues in the global information economy and society through cooperation with other governmental and non-governmental organizations concerned with regional and international telecommunications;

- Promotes the adoption of measures to ensure the safety of life through the cooperation of telecommunication services;
- Promotes, together with international financing and development organizations, the establishment of preferential and favorable lines of credit to be used for the development of social projects aimed, inter alia, to expand telecommunications services in the most remote regions of the country.

The current ITU strategy focuses on a number of strategic issues arising from the rights of the disabled, on the technical design of some accessible standards, providing education and training in information and communication technology accessibility, thus wanting availability to become a reality. In this regard: it encourages sharing of best practices; it offers the possibility of increasing knowledge through conferences and publications; it promotes information security and information space; it promotes bridging the digital divide by building information and communication infrastructure; it encourages emergency communications for disaster prevention and reduction effects.

3.2 Specific actions of electronic warfare

Electronic warfare actions are electromagnetic operations specific to electronic warfare that produce effects in the electromagnetic environment and provide operational support. [6]

These actions are:

- Electronic Surveillance – ES;
- Electronic Attack - EA;
- Electronic Defence – ED.

Electronic warfare is that military action based on exploiting electromagnetic energy to obtain situational awareness and offensive and defensive effects. Together with the conduct of electromagnetic operations, it represents warfare in the electromagnetic environment.

3.2.1 Electronic Surveillance – ES

Electronic surveillance – ES – represents the activity of exploiting the electromagnetic energy for situational awareness and for information gathering.

Electronic surveillance is focused on providing knowledge of the electronic situation at any time and of cues and warnings on the activities of the electromagnetic environment.

Fig. 32 Electronic Surveillance

Electronic surveillance includes monitoring of electromagnetic environment with the purpose of immediate threat recognition in support of electronic warfare operations and other tactical actions such as avoiding threats, directing their weapons to combat and target selection.

Electronic surveillance actions include configuration and allocation of resources for electronic surveillance missions, the modality ofsending the operational commander of data gathered from the electromagnetic environment and using them for tactical decision making.

Information gathered from electromagnetic environment can be considered either signal intelligence or SIGINT, depending on their use. Electronic surveillance information is processed data to the level required for immediate identification or location of the opponent's radiation source. Information obtained by further technical analysis of such data is SIGINT information. Therefore, electronic surveillance can be a source of SIGINT.

On the contrary, the means of electronic surveillance may be based on SIGINT technical data to carry out specific activities.

Basic functions of electronic surveillance (ES) are related to: intercepting, locating, analyzing recognition of hostile radiation sources from the battlefield. It is also very useful and important to note that ES is designed for tactical purposes that require immediate action (real time), in contrast with similar functions of research in general, namely:

- Signals research (SIGINT, Signal INTelligence);
- Electronic research (ELINT, ELectronic INTelligence);
- Communications research (COMINT, COMmunications INTelligence);
- Signals protection (SIGSEC, SIGnal SECurity);

- Radiation research (RINT, Radiation INTelligence);
- Optic research (OPTINT, OPTic INTelligence).

Such information is used to recognize threats and tactical use of weapons or platforms bearing electronic counter measures ECM equipment. ES function is defined as a reaction in real time which makes the necessary distinction between ES receivers and ELINT or COMINT receivers that are used for specific research (intelligence collection) which, generally speaking, involves analyses conducted of intercepted data in unreal time.

ES equipment designed to intercept radar radiation can be divided into two broad categories:

- Radar Warning Receivers (RWR) that work in real time and are used on aircraft, ships, submarines, by land forces for self-protection, etc.;
- Reconaissance Receiver Systems or Surveillance Receiver Systems (RRS or SRS) used for interception, collection, analysis and localization of radar signals in real time.

Future directions of developing ES equipment aim at:

- Increasing the complexity of ES receivers to face an even more complex electromagnetic environment and that is placed in a continuous expansion;
- A massive use of computer techniques for sorting and efficient identification of useful signals.

3.2.2 Electronic Defense – ED

Electronic defense – ED – represents the action of using the electromagnetic energy to protect own and allied forces and the effective use of the electromagnetic spectrum by them.

Electronic Defense – ED represents the actions taken to ensure effective capacity utilization, for self-interest of the electromagnetic spectrum when EW specific means are used by the enemy. ED consists in those passive or active measures taken to protect personnel, facilities or equipment from the effects of enemy electronic warfare actions or friends that reduce, cancel or destroy their combat capabilities. Directed energy weapons DEW are weapons of defense-electronics, when used for defensive purposes. Most modern combat systems using electromagnetic energy from own forces or NATO endowment, have working modes designed to resist the effects of enemy electronic attack.

As with ES and EA components of EW, ED use is a way to obtain a military advantage in a given conflict situation. The essential difference between these components is that, while ED is an integral part of the design or operating methods and means of electronic systems, the ES and EA implementing requires special equipment, operation governed by a number of specific rules.

Naturally, from the definitions accepted for EW components, it results that ED virtually opposes the other two, with different purposes. Therefore, any development or modification of ES and EA technologies involves an immediate reaction from ED technologies and vice versa.

3.2.3 Electronic Attack – EA

Electronic attack – EA – represents the action of using electromagnetic energy, in offensive purposes.

Electronic attack involves the use of electromagnetic energy, of directed energy or antiradiation wepons to attack personnel, facilities and equipment intended to degrade, neutralize or destroy the enemy's fighting ability, being considered a form of "fire". Electronic attack is used to hinder, interrupt, misinform, or prohibit the destruction of command and control capabilities and of the enemy’s fight and to reduce its ability to model and exploit the electromagnetic environment. Electronic attack / EA includes directed energy weapons / DEWs, high power microwaves / HPM, electromagnetic pulse / EMP and radiofrequency devices / RF, having an important role in destroying the opponent through joint operations and combined kinetic and electromagnetic attacks. To ensure maximum efficiency, the performance of an efficient electronic attack is performed only after understanding how to use electromagnetic environment by the adversary.

EA main objectives are the following:

- radar systems;
- radio and radio relay systems;
- navigation systems;
- communication systems, etc.

EA is organized and implemented on the basis of data obtained through electronic research (ELINT) and weapons research.

EA's core missions can be summarized as:

- management disruption;
- neutralization by jamming of the flow of bombing sight spotted by radars and control of air defense systems;
- prohibition, hindering or limitation of the opponent’s electronic research;
- neutralization of navigation working systems;
- destruction and capture of adversary electronic means and systems.

The most common used type is the electronic jamming attack.

This is an action of disturbance destined for total or performant disruption, of systems that process information provided by radio receiver, by other signals from one or more transmitters which use an identical carrier frequency (or very close to the useful signal carrier frequency) or by electromagnetic disturbances that overlap useful information.

Jamming is the major component of EA and consists in applying, at the entry of reception instalations of the media and electronic systems composition of the enemy to be neutralized, of signals with parameters closer to those of useful signals in order to aggravate, prevent and worsen the performance of such equipment or in order to mislead them.

A short classification of jamming may be done as follows:

A) According to its nature:
- natural
- artificial which can be:
    - industrial or aleatory
    - deliberate

B) According to the way of generation, jamming can be:
- active
- passive

C) In terms of the spectrum width, jamming can be:
- of barrage or blocking (of broadband)
- spotted (narrowband)
- sliding (with variable frequency)

D) In terms of oscillation type it can be:
- unmodulated, specific to the beginning of radars period

- modulated, which may further on be:
    - MA (modulated in amplitude)
    - MF (modulated in frequency)
    - MΦ (modulated in phase)
- modulated in impulses, which can be:
    - MA
    - MF etc.

E) In terms of intensity (of spectral density value):
- weak
- medium
- strong

F) In terms of the shape of the directivity characteristic:
- nondirective or omnidirectional
- directive, more efficient in terms of energy etc.

G) According to the intended effect:
- camouflage jamming
- jamming of imination
- neutralization jamming.

Most of the current EA within advanced technology systems are designed to cover the threats posed by both radars operating in pulsed and those in continuous wave. In addition, the high density of threats present at a certain time imposes absolutely and necessarily the existence of a computer capable of performing an efficient allocation (management) of jamming resources (usually limited) available in an EW system.

3.3 Specific Measures of Electronic Warfare

Electronic warfare actions are achieved by applying / using electronic warfare measures that are focused on mechanisms / activities through which electronic warfare acts.

The measures of electronic warfare are:

- Electronic Support Measures – ESM;
- Electronic Counter Measures – ECM;
- Electronic Protection Measures – EPM. [7]

These measures can be used individually or combined to achieve / obtain specific effects of electronic warfare desired magnitude.

3.3.1 Electronic Support Measures - ESM

ESM is the electronic warfare component that contains activities of search, interception, identification and location of electromagnetic emissions in order to immediately recognize threats.

Electronic support measures are a key element of electronic surveillance / ES, representing a source of information that supports the planning and implementation of intelligence and electronic countermeasures, electronic protection measures and other tactical actions.

Electronic support measures include activities carried out in order to know the electronic situation and to immediately recognize threats from the electromagnetic environment in support of operations and other activities at strategic, operational and tactical level, as waning, avoidance of threats and directing weapons to combat them, the process of targets setting and distribution, etc.

Electronic support measures directly support commander at tactical and operational level and participate in providing data and information required at strategic level. When applying measures of electronic support are envisaged the establishment and operational command of ESM technical means, as well as the determination of how data and information are exchanged between electronic warfare forces, on the one hand and between these and other forces, on the other hand.

Components of electronic support measures:

- Communications electronic support measures – targeting electromagnetic signals from media and communication systems;
- Non-communications electronic support meaures – targeting electromagnetic signals from media and non-communication systems.

The characteristics of electronic support measures / ESM are the following:

- They are used during peacetime, in case of armed aggression, when establishing the state of siege, declaring the state of mobilization or war, to develop/update the electronic situation / EOB. During peacetime, ESM actions have the greatest contribution to creating the electronic warfare database necessary to draft future operations;
- Means / systems of electronic support are among the few fighting capabilities specialized in in information gathering at tactical level;
- The means/systems of electronic support ensure the information gathering at tactical and operational levels, continuously, in any weather conditions, to monitor the activity within the electromagnetic environment;
- They exploit the enemy’s electromagnetic emissions and obtain information related to his capabilities and intentions;

- To accomplish the basic mission, the performance of electronic means/systems are based on the passive method of signals interception, except for the operation of own command and control systems;
- They transcend state frontiers.

Information gathering from the electromagnetic environment through electronic support measures represents all searching, interception, identification and location / direction finding activities of electromagnetic signals, within an information area of responsibility or interest so as to obtain primary data necessary for any informational process of the electromagnetic environment.

The activities specific to electronic support measures are:

a) **Search** is the activity consisting in discovering within the electromagnetic environment of electronic means emissions which are of interest;

b) **Interception** is the activity by which the receiving and recording of target electronic means signals is accomplished;

c) **Identification** is the activity through which the receiving and recording of target electronic means/systems signals is accomplished;

d) **Location / direction finding** is the activity that establishes the direction of incoming electromagnetic waves and the site of the monitored targets;

e) **Analysis/evalution** is an activity which involves the processing of data recorded with the aim of identifying and classifying electronic signal sources and identifying their electromagnetic "amprent".

3.3.2 Eletronic Countermeasures – ECM

ECM is the electronic warfare component that includes activities to reduce or hinder the enemy's effective use of the electromagnetic spectrum by using the electromagnetic energy.

ECM includes the electronic jamming, electronic misinformation and electronic neutralization. These countermeasures use the electromagnetic energy for degradation, banning or neutralization, temporary or permanently, of the adversary's combat capabilities.

ECM processes of determining the target, prioritization, selection, classification and establishing the mission do not differ from the targeting process specific to kinetic forces.

ECM specific activities performed by specialized forces, as well as other military actions come in support of Force Commander, directly or indirectly, according to the missions assigned to these forces.

When the electronic countermeasures / ECM are used in the execution of an electronic attack / EA, as a rule, the carrying out of electronic support activities is required in order to provide information about the target and subsequently to assess the efficiency of ECM application and the effects achieved.

Electronic Jamming is the intentional radiation, reradiation or reflection of electromagnetic energy, in order to reduce the efficiency of devices functioning, of the enemy's equipment or electronic systems.

The coordination of actions electronic jamming actions occurs at the highest level of command, but the control of the implementation usually belongs to the tactical level commander.

Electronic jamming actions are successful when receiving sufficient room for manoeuver to be performed both on planned targets and on targets of opportunity.

Electronic jamming coordination is a process that begins in the planning phase of the operation and continues in all its phases.

Electronic misinformation represents the intended radiation, reradiation, the intentional modification, absorption or reflection of electromagnetic energy in order to mislead the enemy forces and means. This takes the following forms:

Electronic misinformation through manipulation. This type of misinformation involves actions to remove relevant exposure cues that can be used by the opponent, and the transmission of false clues.

Electronic misinformation through simulation. This type of misinformation involves actions of simulating own forces capabilities and of deceiving the enemy's forces.

Electronic misinformation through imitation. This type of misinformation induces electromagnetic energy in the enemy electronic systems by imitating their emissions.

The electronic warfare staff provides information about the electromagnetic spectrum by the enemy, the vulnerabilities, surveillance capabilities and their reaction to the electronic misinformation actions carried out by own forces.

Electronic jamming control issues presented above apply to electronic misinformation activities.

Electronic misinformation is vulnerable because it can be detected by the enemy, requiring a special protection in terms of its planning, coordination and execution.

Electronic neutralization represents the deliberate use of electromagnetic energy for the purpose of temporary or permanent damage of the enemy's means which functioning depends on the use of electromagnetic energy.

Electronic neutralization achieved by using directed energy weapons induces a so large amount of energy in the enemy's electronic systems that they become unusable. The electronic neutralization requires visibility directed towards the target and it is influenced by weather conditions – water vapor, dust etc.

Energy directed weapons, as well as other weapon systems, may affect own equipment and systems, if not used properly. Issues related to electronic jamming control above mentioned apply to electronic neutralization as well.

ESM role in the planning and execution of electronic neutralization is to intercept and analyze electromagnetic emissions and to reprogramme systems that are tasked to combat the electronic neutralization weapons of the enemy.

3.3.3 Electronic Protection Measures – EPM

EPM is the electronic warfare component that includes activities to ensure the effective use of the electromagnetic spectrum by friendly forces, in terms of using the same spectrum by foes.

EPM is an essential element in maintaining the commandre's ability to pursue master command and control over equipment and own electronic combat systems. Although EPM is in the responsibility of all users of electronic means and systems, electronic warfare structure is the one to establish the conceptual framework in terms of EPM coordination activities. EPM equipment designed and implemented on combat systems / platforms are designed to improve survival and protection rate of personnel and combat equipment in case of weapons and weapon systems actions that use electromagnetic energy for research, dcontrol and neutralization purposes. Except for protection equipment determined by design and incorporated into combat systems / platforms, the responsibility for implementing EPM is exercised by electronic warfare specialists, with support from managers in charge of spectrum.

In terms of electronic warfare, EPM is the responsibility of command and control structure, exercised in two areas:

- defining measures to ensure the efficient use of EME by own forces;
- developing requirements for the acquisition of equipment to support EPM and staff training who exploits them.

EPM comprises active and passive measures.

Active electronic protection measures are measures detectable by enemy and aim to ensure the effective use of the electromagnetic spectrum by friendly forces.

These may include:

- the change of working frequency, change of modulation type, of repetition frequency and of output power;
- the use of spread spectrum signals;
- re-transmission of a signal using reflectors and repeaters.

Passive measures of electronic protection are undetectable measures, as operating procedures and equipment technical characteristics, meant to ensure the efficient use of the electromagnetic spectrum by friendly forces.

Passive measures of electronic protection include the following actions, without being limited to them:

- reduction of transmitting power at a level sufficient to maintain a connection;
- the use of codes;

- the use of encryption;
- the use of directive antennas;
- installation in locations that minimize the risk of enemy detection and localization;
- SOPs introduction of provisions on limiting the need to communicate and maintain electromagnetic emissions to a minimum level;
- SOPs introduction of provisions related to counteracting misinformation jamming and executed by the enemy;
- Strict measures of emission control / EMCON that prohibit or limit electromagnetic emissions during certain phases of combat;
- the application of technical measures in the design phase of electronic equipment, such as encryption, the emission spread spectrum coherent processing, side-lobe suppression and polarization so as to reduce the risk of being detected.

Emission control. The emission control plan / EMCON is part of the data protection activity and has an important contribution in the action of counteracting the enemy's actions.

Electronic masking is a set of measures aimed at controlled emission of electromagnetic energy on their own frequencies so as to protect their transmitters against ESM activities, without significantly affecting their work.

The objectives in terms of electronic masking are:

- to limit / hinder data and information gathering activities regarding the activities of own electronic systems and means;
- to accomplish enemy misleading by applying the established electronic masking measures regarding capabilities, dislocations or own electronic means and systems intentions;

- to determine reactions that increase the chances of success of activities carried out by own electronic systems and means, according to established missions.

Self-protection measures. Electronic defense applies to protect forces, areas and platforms (e.g. radar and laser warning receivers are passive equipment that can trigger avoidance maneuvers or automatic application of ECM - thermal traps, dipoles etc.).

Combat units require increasingly more electronic warfare self-protection capabilities. The effectiveness of any weapon system is greatly enhanced by the use of electronic devices in order to target or directing fire. These electronic devices can be research radars, communications, active systems operating in the range of infrared waves, laser, airborne transmitters and sensors.

Electronic warfare self-protection systems, thermal traps launchers, electromagnetic obturators – thermal opaque smoke, absorbing paints - can reduce the enemy's electronic warfare effectiveness of systems and means.

Training in the field of EPM must be made during drills and exercises. EPM training must be oriented towards:

- competence development in operating own equipment;
- knowledge of procedures for avoiding intentional and unintentional interferences;
- knowledge of alternative procedures;
- knowledge of selfprotection measures.

All actions specific to electronic warfare can be grouped according to their character in two forms, namely:

- the electronic offensive means to intercept, identify and locate hostile sources of electromagnetic radiation, to use own electronic means and systems for the destruction, neutralization or misleading the enemy's electronic equipment from C4I systems and from weapon systems;

- the electronic defense consists of steps taken to ensure the efficient use of own electronic systems and resources when the enemy uses electronic countermeasures.

3.4 Electronic Warfare Specific Activities

Electronic warfare actions used against targets in the electromagnetic environment produce a wide range of lethal and non-lethal effects. Choosing a capabilitie to develop a course of action of electronic warfare takes into account the desired effect on the target, as well as other considerations, such as, for example, the action time or the limitation of collateral damage.

Electronic warfare capabilities provide options to meet their targets, during combat actions there may be situations where it is desirable to limit physical damage on a target, in these circumstances electronic warfare capabilities can be used to obtain non-lethal or lethal effects on target. The capabilities of electronic warfare units are used to obtain non-lethal or lethal effects to ensure freedom of action and control of electromagnetic environment while simultaneously prohibiting its use by the enemy.

How to use electronic warfare capabilities. Electronic warfare capabilities can be used from air, land and sea combat platforms, and in space, with /without pilot, controlled or uncontrolled. Without a proper coordination and integration, the use of electronic warfare capabilities could adversely affect the operations carried out by own forces.

Examples may include fratricide in the electromagnetic environment or the destruction of high-value informative targets.

The effects of electronic warfare actions:

Detection is achieved by passive and active monitoring of the operational environment in order to identify threats from the range of radio waves, optical, laser, infrared, acoustic and ultraviolet ones. Situational awareness from the electromagnetic environment is the first step so as the exploitation, target selection, defense planning and protection force to be effective. Own forces must have the necessary capabilities for detecting and determining the type of intentional interference caused by electronic attack, of unintentional interference or of effects determined by environment on the normal operation of own / allied electronic systems and means.

Prohibition/Banning is obtained by controlling the information that the enemy receives from the electromagnetic environment and preventing the acquisition of accurate information about own forces. It can be obtained after carrying out of specific electronic warfare actions.

Electronic **deception** is achieved by creating confusion or false information inducing on the enemy through the electromagnetic environment. Through electronic warfare actions the enemy's decision-making process is manipulated, creating him difficulties in knowing the correct reality.

Reduction in the electromagnetic environment is achieved by using techniques that diminish the enemy's ability to use the electromagnetic spectrum, negatively affecting the combat effectiveness.

Interruption in the electromagnetic environment is achieved by using capabilities that produce interferences on the enemy's electronic warfare capabilities, in order to diminish his combat effectiveness.

Destruction represents the elimination of the enemy's combat capability. C2 sensors and nodes are important targets, and their destruction significantly influences the enemy's perception and ability to coordinate his actions. The electronic warfare, through electronic surveillance actions, supports physical destruction by providing target location and information about it.

Protection within the electromagnetic environment represents the use of electromagnetic energy or of capabilities based on it, to protect own forces and means against the enemy's offensive actions or of capabilities based on it to protect own forces and means against the enemy's offensive actions within the electromagnetic environment.

Neutralization. In the context of electronic warfare, neutralization represents the deliberate use of electromagnetic energy to temporarily or permanently deteriorate the enemy's electronic devices, whose functioning is based exclusively on the use of electromagnetic energy. The use of energy guided weapons represents the direct contribution of electronic warfare to the destruction of the enemy's electronic equipment.

BIBLIOGRAPHY

[1] ALBERTS, D. S., GARSTKA, J. J., HAYES, R. E. and SIGNORI, D. A. (2001). *Understanding Information Age Warfare*. CCRP Publication Series.

[2] ALBERTS, D. (2005). *Power to the Edge: Command...Control...in the Information Age*. CCRP Publication Series.

[3] ALBERTS, D. S., HUBER, R. K. and MOFFAT, J. (2010). *NATO NEC C2 maturity model.* CCRP Publication Series.

[4] VIZITIU, I. C. (2005). *Electronic Warfare. Fundamental Notions*. Bucharest : A.T.M. Publishing House.

[5] „Wikipedia, the free encyclopedia" [Interactive]. Available at: http://en.wikipedia.org/wiki/James_Clerk_Maxwell#Electromagnetism. [Accessed: 19th August, 2014].

[6] VIZITIU, I. C. (2008). *Electronic Warfare. Modern Aspects*. Bucharest : A.T.M. Publishing House.

[7] ADAMY, D. (2004). *EW 102: a second course in electronic warfare.* Horizon House Publications Inc.

[8] ADAMY, D. (2009). *EW 103: Tactical Battlefield Communications electronic warfare*. Artech House Inc.

[9] ALBERTS, D. (2000). *Network Centric Warfare: Developing and Leveraging Information Superiority*. CCRP Publication Series.

[10] SMITH, E. A. (2000). *Network Centric Warfare: Where's the beef?* Naval War College Review.

[11] GHERMAN, L. (2010). *Warfare in the Information Age*. Journal of Defense Resources Management, no. 1.

[12] MACCUISH, D. (2012). *Orientation: key to the OODA loop – the culture factor*. Journal of Defense Resources Management, no. 2.

[13] TOPOR, S. (2004). *Information War. Course notes*. Bucharest : U.N.Ap. Publishing House.

[14] VIZITIU, I. C. (2011). *Electronic Warfare. Theory and Appliations*. Bucharest : A.T.M. Publishing House.

[15] GHERMAN, L. (2013). *Information Age view of the OODA loop,* Review of the Air Force Academy, no. 1.

[16] GHERMAN, L. (2011). *The Second Revolution in Military Affairs.* Journal of Defence Resources Management, no. 1.

[17] ADAMY, D. (2001). *EW 101: A First Course in Electronic Warfare*. Artech House Inc.

Title: **ELECTRONIC WARFARE IN THE INFORMATION AGE**

Textbook

Authors: Laurian GHERMAN, Cosmina Oana ROMAN, Marcel HARAKAĽ
Publisher: Armed Forces Academy of General M. R. Štefánik, Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic
Edition: 70 copies
Pages: 102
Printing: First, 2015
Format: B5
Printed by: Armed Forces Academy of General M. R. Štefánik, Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic
Design: Robert KANDRIK
Year of issue: 2015

ISBN 978-80-8040-512-0