ELECTRONIC WARFARE IN THE ARMED FORCES OF THE REPUBLIC OF POLAND AT THE TURN OF THE 20TH AND 21ST CENTURY

Waldemar SCHEFFS
National Defense University, Warsaw, Poland

1. A Summary:

The political changes that took place in Poland in the 1980th began the process of shaping and adjusting the Polish economy and society to the new realities and freedoms resulting from the democratic life.

However, simultaneously they enforced the transformation of the Polish Armed Forces, which from the army prepared for performing offensive operations started to be remodeled into an army ready to operate in different environments and conditions, as well as in various geopolitical situations. The process of change progressed gradually.

The specified goals were accomplished by small steps and one might say that the process continues.

The article is characterized by a historical approach and its purpose is to present the general aspects of the Electronic Warfare (EW) changes in the context of the Polish Armed Forces, concentrating on the quantity and types of the electronic combat military units, as well as on the changes concerning the theory of the Electronic Warfare, which resulted from its transformed character.

The subject of this article are the results of the comparative researches, obtained as an effect of solving the problem defined in the form of a question:

How was the development of the Electronic Warfare shaped in the field of the Polish Armed Forces at the turn of the 20th and 21st century?

In order to find the solution of the main problem, it was necessary to define in detail the issues related to using the electronic combat units during military operations in three time intervals: years before the political transformation, period of time just before Poland joined NATO and time immediately after this event, and, finally, the first decade of the 21st century, when dramatic theoretical, organizational and procedural changes could be observed.

After the Second World War, the Polish Armed Forces were formed through integrating various military formations fighting on the Western fronts and the Polish army fighting together with the soviet armies on the Eastern front. Thus one single organism was created.

It must be emphasized that the number of the soldiers from the armies operating in the West comprised a very small percentage of the whole newly formed People's Army of Poland. It had at its disposal military equipment which was almost entirely produced in the USSR.

For the training purposes Polish regulations and doctrines were used. However, all of them were written in accordance with the soviet politics.

It was not earlier than during the political transformation in Poland that the army underwent some changes. The number of the soldiers was reduced from 450,000 (near the end of the 1980th) to 200,000 around the end of the 20th century.

At the time being, there are 120,000 soldiers in the Polish Armed Forces, including the National Reserve Forces.

Also, the amount of the military equipment was reduced, mainly the armored and mechanized. The first military units which started the modernization process aimed at achieving the level comparable to the NATO member states' armies are the intelligence units, the Special Forces in particular. Even before Poland joined the NATO, the Special Forces units had been training together with the NATO units and had been provided with the equipment purchased under the support program prepared by the NATO member states. Polish Special Forces were also able to implement doctrinal solutions in the field of reconnaissance, such as e.g. IPB (Information of Prepared of Battlefield). The series of changes involved also the Radio Electronic Warfare units and here not only their structure was transformed, but also the definitions related and the essence of the Radio Electronic Warfare (REW).

Finally, the summary of this article presents new development directions of the Electronic Warfare, possible to follow not only by the Polish Armed Forces, but also by the armies of the other NATO member states. The whole material presented below is based on conclusions drawn from the specialist literature analysis, which the author supplemented with results obtained from employing methods of direct observation.

2. Electronic Warfare before the political transformation

In order to characterize the transformation of the Radio Electronic Warfare within the Polish Armed Forces, one must go back to the Second World War and the time directly after its end, since it was then that the REW became explicitly divided into three types of operations – directed from the ground, sea surface and air.

This partition enforced directly the organization of the REW units.

The Western states concentrated on developing and modernizing the air units mostly, while the East preferred rather to invest in the land forces.

The Western countries developed mostly Radio Electronic Warfare systems to be assembled on planes and ships, which was the result of the Second World War experiences and the higher development level in the context of the electronics and technologies. At the same time, the states that had formerly signed the Warsaw Pact (and were at the time of the cold war the opponents of the West) developed the Radio Electronic Warfare applicable for the land forces, which was also dictated by the size of the mechanized and panzer armies.

While improving the technique and forms of leading Radio Electronic Warfare operations[1] often the experiences resulting from foreign local wars were used: Korea (1950-1953), Vietnam (1964-1973), Middle East (1967, 1973, 1981), Falklands conflict over the Malvinas (1982), the Persian Gulf (1990-1991, 2001), Yugoslavia (1999).

The military conflicts mentioned above have shaped the contemporary character of the REW. In the West, operations led in the environment of the electromagnetic waves started to dominate the air and marine combat operations, but in the East the Electronic Warfare appliances were used mostly in the land environment and only sometimes during air or maritime operations.

Only the Armed Forces of the USSR maintained the whole possible arsenal of the REW equipment in every type of armed forces.

The proportions concerning the amount and type of the REW equipment are perceptible until now. Such a differentiated approach to the REW systems resulted from the Second World War experiences, a sudden development of science and technologies at the West and the beginning of the arms race. Both the USA and the remaining NATO member states aspired to achieving the possibility to use advance military measures in every place of the globe, and that is why they needed systems able to detect and identify an opponent from a very long distance.

[1] The notion of the electronic combat was shaped in the 1950th and 1960th. Before, the term „radio war" was used. The phrase „radio war" appeared both in the Eastern and the Western literature. Over time, the NATO states started to use the notion of the „electronic warfare", while the Eastern countries preferred the term Radio Electronic Combat. This situation was changed later by the doctrine concerning the Electronic Warfare, created by the Polish Armed Forces in 2003.

The dominating role in this context could be played only by the long-distance surveillance aircraft, since electronic intelligence from the space was at that time only vaguely considered and ten years had to pass when this idea could be implemented.

In that period of time, the strategic air intelligence of the USA Air Force determined the development directions concerning the electronic combat devices.

Very intense intelligence actions combined with jamming and, as well as maintaining radio contact in every part of the globe is the basis of developing new technologies in the field of Electronic Warfare.

The electromagnetic environment, or – in more general terms – electronic – became the obvious domain of the silent combat arms race.

At that time, the Polish Armed Forces operated on the basis of the offensive doctrines, according to which the actions concerning the REW were focused on radio electronic interaction mainly with the land opponent. One of such tasks was destroying the radio electronic devices of the opponent by means of firing assets.

It could be performed by the aviation, artillery or combat units.

A proper coordinates necessary for such operations were received from the intelligence systems, both national and cooperating (allied).

3. First changes at the end of the 20th century

After the period of political transportation, the intelligence forces underwent a process of integrating the electromagnetic intelligence units with the units responsible for radar and radio frequency interferences. A single element was formed – Radio Electronic Warfare.

There were a few arguments for such integration. One of them was the need to keep all the radio electronic information in one decision-making center, where the current situation would be evaluated and the needs of firing radar operations could be met.

In many units dealing with intelligence and the radar and electronic countermeasures the same type of equipment was used for performing the same tasks, which resulted in unnecessarily doubling actions, while the time of the information flow within the intelligence system caused too long period of time in the context of waiting for the decisions to be sent to interaction means.

It was also the time when the related definition and its elements changed into: “Radio Electronic Warfare (REW) means military operations and actions during which electromagnetic energy is used in order to identify and disorganize the radio electronic systems of the opponent and create conditions allowing the own analogical systems for stable work.”[2].

The *REW* was divided into the following elements: electromagnetic intelligence, suppression and defense.

Such a situation lasted till 2003, when a new doctrine concerning the Electronic Combat was introduced.

Poland belonged then to the NATO already, therefore it is easy to deduct that it took six years to transform the REW doctrine into the EW doctrine.

Such a long period of time was necessary to re-organize thoroughly the structure of the REW units.

Until joining the NATO, Polish army was characterized by the *REW* battalions on the army level and later on the corps level, as well as the independent regiments responsible for radio and electromagnetic intelligence, as well as for radio and electronic countermeasures.

After the first re-organization of the PAF, when some of the army structures were eliminated, the army radio-electronic battalions were subordinated to the radio-electronic intelligence regiments.

At that time, two such regiments were formed, along with the 8th radio jamming regiment, and 11th radio-electronic intelligence regiment.

[2] *Principles of preparing and conducting the radio electronic battle by the PAF*, Szt. Gen, Warsaw 1995 p. 5

The 10th radar recognition regiment and the 4th radar jamming regiment were dissolved, while the 9th radio-electronic intelligence regiment was moved to Lidzbark Warmiński. Simultaneously, after a complicated period of re-organization the National Defense Forces were integrated with the Air Forces into the National Air Defense Forces.

Table 1. Numbers and types of the REW units in the Polish Armed Forces before the political transformation

Type	Location	Affiliation
1st radio-electronic intelligence regiment	Grójec	Air and Air Defense Forces
2nd radio-electronic intelligence regiment	Przasnysz	Land Forces
3rd radio-electronic jamming regiment	Lidzbark Warmiński	Air and Air Defense Forces
4th radar jamming regiment	Giżycko	Land Forces
5th special communications battalion		
6th radio-electronic intelligence regiment	Gdynia	Navy
7 th radio intelligence regiment of Military Police	Skierniewice	
8th radio jamming regiment		Land Forces
9th radio-electronic intelligence regiment	Biała Podlaska/ Lidzbark Warmiński	Land Forces
10th radar recognition regiment	Dziwnów	Land Forces
11th radio-electronic battalion	Zgorzelec	Land Forces
12th radio-electronic battalion	Kołobrzeg	Land Forces
15th radio-electronic battalion (only professional soldiers – with out conscripts)	Biała Podlaska	Land Forces

Source: http://www.serwis-militarny.net/forum/viewtopic.php?f=18&t=11484 [access 02.03.2015]

This structure included two regiments – one radio-electronic intelligence regiment and one radio-electronic jamming e regiment, which in 2000 were transformed into the 2nd radio-electronic battalion. At that time the Navy was provided with one radio-electronic regiment. All these transformations and reductions carried out within Polish Armed Forces resulted in the fact that by the end of the 20th century on the strategic and operational level the military units functioned within the regiment structure, while on the tactical level there were REW companies combined with the electronic countermeasures elements in all types of the forces.

4. Electronic Warfare before of the new century

The period immediately after Polish Armed Forces joined the NATO was characterized by intensified implementation of new procedures concerning the command, intelligence, REW and adapting the old and new equipment to the NATO requirements.

It must be emphasized that this process was not smooth in every case.

A lot of time was spent on discussions and reaching agreements, as well as understanding the philosophy underlying the changes to be introduced.

Many officers and privates were forced to learn new theory, which had to be turned into practice through command and staff exercises and trainings with the troops, to be used later during everyday work according to new procedures within the new staff structures.

According to the doctrinal assumptions of the 2003, the dominating environment for the Electronic Warfare was the electromagnetic environment, where the combat was carried on by all types of the armed forces.

It was of the universal character, which meant that all units were to participate within the scope of their competencies. The main effort of such operations rested on the specialized units equipped with electronic intelligence, electronic jamming and radio electronic defense devices.

The EW functions in the electromagnetic environment, which means that “the environment of the EW is the three-dimensional space in which the electromagnetic waves radiate from the radio electronic devices and are absorbed by some other appliances”. Hence, the electromagnetic environment is characterized by: scope of the spectrum of the electromagnetic waves which is used, density of the used frequencies, density (power) of the EM energy within the space, density of the radio electronic (RE) devices per square kilometer (W/km^2), arrangement of the deployed RE devices and their distance from the military line of the troops, listing and deployment of the important RE objects (mostly communication, radar posts, electronic jamming stations, RE intelligence centers, satellite communications terminals, intelligence and radio navigation posts etc.).

The EW is conducted on the same frequencies which are used by the radio electronic systems of the opponent's forces (including communications, radars, remote sensing, and radio navigation). These are frequencies from 30 kHz to 40GHz (but also 94-108 GHz), as well as infrared.

Apart from that, the EW staff cells continuously update the lists of the important RE objects assigned for intelligence and jamming, which allows for immediate identification of a given object along with its probable location, to be followed by prompt electronic attack. These actions are performed in order to direct the RE detection, define the optimal time of the jamming or conducting electromagnetic or fire attack.

The purpose of the EW within the framework of various tactical and operational actions of the forces is to acquire information on the electronic devices and systems of the opponent’s army (land forces, air and anti-air defense, strike aviation, navy and space forces).

The next step is the electronic attack. Another equally important aim is disorganizing the work of the opponent's combat management systems

The environment of the electromagnetic waves (EMW) successively starts to be dominant in the combat environment. One could enumerate a lot of weapon systems, in which the electronic devices supporting the military operations play the leading role in the EMW environment.

The most important of them are the following:

- command and communications systems (C2W, Jaśmin, Szafran, Łowcza, Podbiał);
- radar command systems (Dunaj, Loara);
- weapons management and directing systems (missiles, UAV etc.);
- intelligence systems (e.g. acoustic Pilar Mk II, optoelectronic military observation towers Kobuz, military detection and supervision system MDSS);
- Suppression of Enemy Air Defenses (SEAD);
- EW systems (e.g. Przebiśnieg, Kaktus, which also include the EM impulse);
- IT systems (cybernetic, e.g. BITcom, Złocień, Służba);
- navigation systems (GPS, Glonass)
- different supporting systems of the air forces, land forces and the navy.

According to the approach presented here, the electronic devices of the EW systems work uninterruptedly during the peacetime, crisis and war, and only, depending on which period is concerned, if necessary, the scope and intensity of the electronic activity of military character and significance grows.

This approach is task-oriented, which means that the operating both of the EW system and the theory concerned within the PAF applies to precisely defined tasks. During peace time the military staffs prepare for operating within the defined time and space framework. These experiences later translate into concrete solutions during the exercises.

The officers (planners) of the EW cells analyze the actions of the opponent, evaluate the threat, plan concrete operations, conduct them and then examine the effects (through signals emitted after the military action by the opponent's electronic devices, in all frequencies). If the operation proved to be successful, then the next step follows, and of not, the operation is repeated or the formerly made decision is verified and a modified course of action is taken. This general regulation of planning and operating (plan – operate – evaluate – verify), which was historically shaped, proved to be successful in every army involved in EW actions.

5. Electronic Warfare at the beginning of the XXI century

The beginning of the 21st century brought consecutive theoretical, procedural and organizational changes for the EW units of the PAF. The doctrine implemented in 2003, which was mentioned above), resulted in slightly altered approach towards the EW theory and practice. Apart from changing the name of this warfare itself, into the Electronic Warfare, a new definition was introduced: “The Electronic Warfare means military operations involving identification of the opponent's sources of electromagnetic emission, disorganizing the working of his electronic devices and systems using the EM energy, including the beam energy, simultaneously providing the conditions for effective usage of such waves by one's own forces”[3].

This definition is already completely in accordance with the one that is in force within the NATO structures. In addition, the subdivision of the EW also changed into: electronic intelligence, electronic countermeasures and electronic defense. These assumptions made suggest explicitly that we enter a period when we have to take into account not only the possibility of typical radio or radar jamming, but that from now one more focus should be put on the pulse and directed EM energy interactions. That is the purpose of the reorganization of the EW units. Fire attack, emphasized so strongly in the context of the previous definition, although effective, becomes limited to striking with the precision guided munitions.

The assumptions made indicate that the EW is characterized by two main streams:

Offensive – active influencing the electronic devices of the opponent by using the operational intelligence and electronic countermeasures;

Defensive – creating environment suitable for undisturbed operating of one's own electronic devices, so that they could fulfill the function they were appointed on the battlefield.

However, since 2004 the Polish EW theory mentions a third stream (called reconnaissance stream at that time),[4] characterized by achieving the EM information about the currently operating electronic devices and systems of the opponent in a complex way. In addition, it assumes monitoring the magnetic fields, resilient waves, power-driven courses (electric signals) within the IT webs, and by analyzing this data (character and direction these signals come from) determining all possibilities of using this information for the intelligence purposes.

The second stream was aimed at complex and active influencing the electronic devices of the opponent in order to disturb or disrupting their operating, or even destroying them. The goal of the thirds stream was creating safe environment for one's own electronic systems so that they could work undisturbed.

This meant securing the process of gathering, processing and distributing electronic data. The further step would be blocking the electronic devices of the opponent and not allowing them for collecting and sending information, as well as damaging them.

[3] *Electronic Warfare*, Szt. Gen., Warsaw 2003, p. 7.

[4] W. Scheffs, *Electronic Combat during the peace-supporting operations*, National Defense Academy (AON), Warsaw 2005, W. Scheffs, *Electronic Warfare system during the crisis operations*, National Defense Academy (AON), Warsaw 2006, W. Scheffs, *Electronic combat during the asymmetrical operations*, National Defense Academy (AON), Warsaw 2007.

Development of the EW within the PAF was determined by another reorganization of the EW units, which started at the beginning of the 21st century and lasted until 2007.

Implementation of the new doctrine resulted in disbanding the radio-electronic intelligence regiments, which were replaced with Radio Electronic Intelligence Centers, one for each type of the armed forces.

The tactical level is more stable and did not changed, while the EW unit remained as a company. During peace time the EW company is trained within the structure of the radio-electronic battalion[5], which was created on the basis on the 8th radio jamming regiment. During the training the company is delegated to one of the divisions. At the beginning of the next decade the 8th regiment was included into the structure of the Radio Electronic Intelligence Centre.

The Air Force underwent similar changes[6], which also meant disbanding of the radio electronic regiments and creating the Radio Electronic Intelligence Centre. At the beginning, two radio-electronic battalions became compliant with it, but they were disbanded in 2007 as well and this was when the Radio Electronic Intelligence Centre's structure was transformed to the level of the company. In a similar way, the radio electronic regiment of the Navy was transformed into the Radio Electronic Intelligence Centre.

The new structures fulfill the modular assumptions concerning the task forces, within which proper EW forces are to be appointed and directed from the Radio Electronic Intelligence Centers in order to perform a given task. If necessary, it may be even a radio-electronic battalion.

6. EW – towards new challenges

Since 2007 the member states of the North Atlantic Treaty Organization started to reconsider the ideas concerning the EW, which lead to initiating the process of changing the general concept of the EW and updating the EW doctrines[7].

The modification which has been thus triggered off is indispensable mainly because of two factors: re-defining of the combat field threats, which have appeared ever since the break-up of the Yugoslavia and adjusting the EW to the requirements of the future military operations to be conducted by the NATO forces. The previous document defining the EW policy – MC 0064 – NATO *Electronic Warfare Policy* – was replaced by a new version MC 0064/10, which delineated the basic notions related to the EW and indicates its development directions. Simultaneously, this document contains the requirements for the future EW systems. The new definition goes as follows: „Electronic Warfare is military action that exploits EM energy to provide situational awareness and achieve offensive and defensive effects”[8]. At the same time, this new definition introduces new notions[9]: Electronic Intelligence (EI) – use of the EM energy to provide situational awareness and intelligence[10]; Electronic Attack (EA) – use of the EM energy for offensive purposes; Electronic Defense (ED) – use of EM energy to provide protection and to ensure effective friendly use of the EM spectrum.

Such form of the new document MC 0064/10 prove that the above-mentioned definitions have been introduced in order to highlight the new character of the EW forces, which is equal to implementation if the idea concerning the Effect Based Approach to Operations (EBAO)[11].

[5] The 8th radio electronic combat battalion kept the old name of the radio electronic combat.

[6] As a result of the transformation of the Air Defense Forces the Air Forces were established. This name was in use since July 1, 2004.

[7] The process of changing the NATO EW idea described here started in 2007 and it was initiated by a review prepared by the NATO Electronic Warfare Advisory Committee (NEWAC), entitled Concept for the Future NATO Electronic Warfare and Related Disciplines.

[8] *MC 0064/10 – NATO Electronic Warfare Policy*, NEWAC, 2008, p. 3.

[9] Ibid. p. 3.

[10] Instead of the term Electronic Intelligence Polish authors often use the notion of the Electronic Guarding.

[11] The EBAO concept in the context of the EW assumes, among others, expanding teh field of activity related to EW and introducing not only new definitions for the so-far existing EW elements (EI, EA and ED), but also a new element - Electronic Warfare Management (EWM). It assumes management of the spectrum, data links and data bases, functioning of the Signals Electronic Warfare Operations Centre (SEWOC), creating the EOB etc. See: *Concept for the Future NATO Electronic Warfare and Related Disciplines*, NEWAC, 2007, p. 8. More about the new NATO EW concept in: D. Kołasiński, K. Dymanowski, *Changing WE Concept within the NATO*, in: „Przegląd Sił Powietrznych” (Polish Air Force Review), No. 11/2009, pp. 4-13.

Therefore, it is easy to notice that such so-far used definitions of the EW elements as Electronic Warfare Support Measures – ESM; Electronic Countermeasures – ECM; Electronic Protective Measures – EPM, are of a narrower character and subordinate to the new ones: Electronic Intelligence (EI), Electronic Attack (EA) and Electronic Defense (ED).

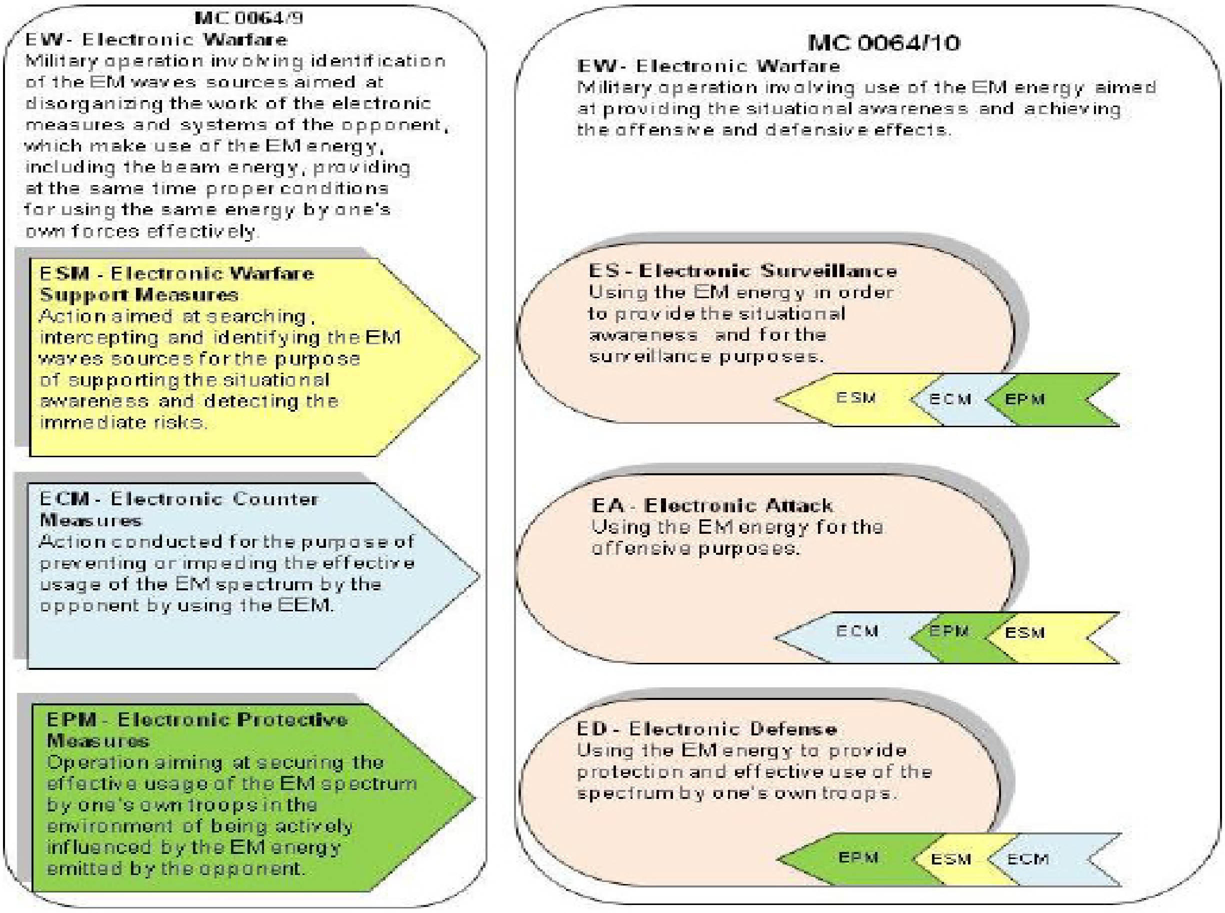
MC 0064/9
EW - Electronic Warfare
Military operation involving identification of the EM waves sources aimed at disorganizing the work of the electronic measures and systems of the opponent, which make use of the EM energy, including the beam energy, providing at the same time proper conditions for using the same energy by one's own forces effectively.
ESM - Electronic Warfare Support Measures
Action aimed at searching, intercepting and identifying the EM waves sources for the purpose of supporting the situational awareness and detecting the immediate risks.
ECM - Electronic Counter Measures
Action conducted for the purpose of preventing or impeding the effective usage of the EM spectrum by the opponent by using the EEM.
EPM - Electronic Protective Measures
Operation aiming at securing the effective usage of the EM spectrum by one's own troops in the environment of being actively influenced by the EM energy emitted by the opponent.
MC 0064/10
EW - Electronic Warfare
Military operation involving use of the EM energy aimed at providing the situational awareness and achieving the offensive and defensive effects.
ES - Electronic Surveillance
Using the EM energy in order to provide the situational awareness and for the surveillance purposes.
ESM
ECM
EPM
EA - Electronic Attack
Using the EM energy for the offensive purposes.
ECM
EPM
ESM
ED - Electronic Defense
Using the EM energy to provide protection and effective use of the spectrum by one's own troops.
EPM
ESM
ECM

Fig. 1. Comparison of the EW definition and its elements in the subsequent versions of the MC 0064 document. *Source: own materials.*

Electronic Warfare Support, Counter Measures and Protective Measures, as well as other military measures conducted within the EM environment (radio communication, microwave transmission, radar communication wave, radio navigation and others), can be integrated during one single operation (performing a specified task). The principal and superior goal of such an operation (informative, offensive or defensive) shall determine, which of these components shall dominate, qualifying thus the operation to one of the main fields: EI, EA or ED (see fig. 1).

The new NATO EW concept (MC0064/10) is explicitly influenced by the ideas presented in the American EW doctrines. Such an impact of the American thoughts should not surprise anyone, since the US Armed Forces lead in the field of introducing new technologies and military ideas, not only in the context of the EW, but of the other forces as well. At the same time, the US army has the greatest military experience, which is the result of the recent military conflicts.

The new EW concept assumed increase of the offensive character in every type of operation. This included possibility of using the EW for attacking not only the equipment and infrastructure, but also its personnel of the opponent (which is a novelty in comparison to all the previous EW concepts).

Also, such an approach allows the commander of a given level to command directly all the EW Support Measures subordinate to him[12].

[12] K. Dymanowski, *Electronic Warfare in the Air Forces…*, Ed. quot., pp. 82-83.

At the time being, the planners must at first define the desired effect of conducting the EW in the EM environment and its influence on performance and success of the whole joint operation. It enforces to take up a new approach towards the planning, preparing and conducting the EW – an approach which would exceed the current framework.

According to the old formula, having at one's disposal a given amount and types of the EW equipment, evaluation of the possibilities concerning influencing the electronic potential of the opponent would be followed by just rough estimation of the effect, assuming repetitiveness of the actions until achieving the desired effect.

The new approach allows for defining the desirable objectives, to which the amount of the necessary equipment, methods of operating and structure are adjusted.

If any NATO member state, its army or one of the military levels lacks the necessary EW potential, then a support of the NATO forces is provided. Therefore, according to the new EW formula the basis of conducting EW are the joint operations, which shall be the basis of the future actions taken up within the EM environment.

The theoretical WE assumptions of the new doctrine have been expanded by applying an innovative attitude represented by R. Elder.

Apart from the three typical EW components, the R. Elder one more element – the EM spectrum control, which is to be achieved by means of successful management of one's own electronic systems and coordinating their work, applying at the same time counter measures towards the analogical systems of the opponent[13].

In my opinion, the EM spectrum control should rather be the *goal* of the EW than its component. And such a goal can be accomplished just by skillful managing the EW forces and proper coordination of their operations.

Therefore, I do not share the opinion according to which we control the spectrum and manage the frequencies on which both we and the opponent operate.

The new EW doctrine AJP.3.6. also assumes managing the EW by: administering the EM spectrum, data links and bases, the EM environment, EW databases, coordinating the EW through Electronic Warfare Coordination Cell (EWCC), Signals Electronic Warfare Operations Centre (SEWOC), managing the EW potential through the supporting military staff, managing the map of the electronic situation.

Another very important field of EW activity is coordinating the EW tasks with the operations involving influencing the computer networks - Computer Network Operations (CNO), Civil-Military Cooperation (CIMIC) and informing the public opinion about actions which, according to the NATO and US approach, are not a part of the information operations, but are closely related with them[14]. Quite a serious problem if the correlation of the EW during operations conducted on the borderline of crisis and war or Peacetime and crisis. Such activities often involve participation of civilian institutions, media, non-governmental organizations (NGOs), religious institutions of different religions and churches themselves.

Almost all of them use the systems and devices emitting the EM waves on a large scale, for the purposes of communicating and transmitting TV and radio signals.

Therefore, it is necessary to coordinate the usage of spectrum by the military and civilian bodies. Such activities are strongly emphasized in the American EW doctrine.

It also stresses the necessity to prepare proper procedures concerning the electronic interference. Some NATO documents also accentuate the role of the civilian and military electronic systems and devices operating together during joint operations.[15] The main purpose of such coordination is to prevent errant jamming of the electronic devices and systems working for civilian institutions and other neutral organizations.

[13] R. Elder, *21st Century Electronic Warfare*, Association of Old Crows, 2010, pp. 1 and 6.

[14] See K. Dymanowski, *Electronic Warfare in the Air Forces…*, Ed. quot., p. 86.

[15] W. Scheffs, M Łokociejewski, *Electronic Warfare in operations and combat*, National Defense Academy (AON), Warsaw pp. 75-79.

Already since the beginning of the 21st century the process of developing the new EW theory initiated in the Polish Armed Forces have been leading to gradual replacement of the old EW equipment with new elements. At that time, the EW units of the tactical levels became equipped with the new Przebiśnieg system, of a highly mobile character and capable of instant reception and detecting all types of modulation used then.

In addition, a new system called BREŃ was implemented and it was assigned for identifying the radar signals. Both systems went through numerous modernizations when the new implementation process of the new EW doctrine has started, they proved to be a modern equipment basis ready to perform identification and jamming tasks on the tactical level and in accordance to contemporary military requirements.

However, the equipment modernization was not limited to the land forces. The most serious equipment replacement took place in the Air Forces. Apart from the modern F-16 planes and EW systems produced especially for this type of the aircraft, all the equipment produced in the USSR was replaced. Due to many international contracts and the fact that Poland has joined the NATO, Polish army gained access to the newest intelligence technologies and the equipment was bought from such companies as Rohde&Schwarz or Thomson.

Radiolocation recognition stations were modernized and the MSW-R station started operating, replacing the Gunica system. An automatized identification system Wołczenica. Was introduced. These are just the main systems that started working in the PAF and which meet the standards of the new EW doctrine, which is being implemented right now. In the nearest future another EW system KAKTUS shall be introduced on the operational and tactical levels, very modern and completely compatible with the equipment of the allies. Polish Armed Forces face challenges related to mobility and speed of operating, which directly influences the effectiveness. The EW units must provide undisturbed flow of the information from every location, where the combat units operate, which is absolutely essential for the effectiveness of the operations. It is an important requirement, but is it the most important one? Another one that the PAF will soon have to meet is related to the activity of the EW units within the computer networks.

Contemporary combat operations are frequently transferred to the virtual world, where the soldier shall soon be just the effect of the action. The tools used here mean specialized equipment and the man, being a component of the system, must be able to operate it, often operating from far distance, but effectively. The few experiences gained during the peace and stabilization missions in Iraq or Afghanistan are not sufficient. At the moment, solution to this problem is being sought for by the military decision makers.

It is always unclear what the future shall bring, but already now we have to get prepared for this, what might happen. The new EW theories implemented now must serve not the current situation, but the future operations. The equipment introduced now is already outdated, and while designing new devices, we must concentrate on the future. Hence the immense importance of the specialized knowledge and imagination, which shall together create new images of operating.

The growing meaning of the electronic and IT indicate future joint operations conducted in different types of the environment. Asymmetrical and network-centric activities are just a part of the future operations conducted by the modern EW. The cyberspace which has not been explored may entail serious risks. The attacks directed towards government internet network that have been revealed in Latvia and Georgia prove without doubts that the role of the virtual world is increasingly important and the fight takes place within the computers, the weapon being the bits of the IT programs.

Who is going to win this fight? At the moment, there is no answer to this question, although the adversaries of the new concepts shall say that the winner is always this party which is first to choose the location and weapon.

But what would happen if the opponent was prepared for the attack, because he had been monitoring the situation beforehand?

The IT answer can bring catastrophic effects for all the people, not just those directly engaged in the conflict.

These effects may spread to other countries. Parodying the words of the famous s-f writer, Stanisław Lem, who wrote, that „…the future war shall be atomic, and the next one shall be the waddy war”, I could say today, that first there is going to be the bits war, and then the waddy war.