THE AUTOMATION OF ELECTRONIC EQUIPMENT IN CYBERSPACE AND ELECTRONIC WARFARE

AUTOMATYZACJA DZIAŁAŃ URZĄDZEŃ ELEKTRONICZNYCH W ŚRODOWISKU CYBERPRZESTRZENI I WALKI ELEKTRONICZNEJ

Waldemar Scheffs

National Defense University, Akademia Obrony Narodowej
w.scheffs@aon.edu.pl

Abstract: *The rapid technological advancement of IT engineering has given rise to clandestine and intense war in the electromagnetic and IT environment. A signal transmitted simultaneously to a large number of receivers has become a tool to wage this kind of war. The signal itself is devoid of power and mass. New technologies have given rise to new potential areas of warfare. Cyberspace is the most telling example of an artificially created environment. This new warfare environment has been claiming an ever larger proportion in the ways of sending and receiving information command, reconnaissance electronic war, among many others. The article mentions topics closely connected with the automation of electrical devices operating under two different conditions: cybernetic and electromagnetic. One dovetails with the other and both could use the same type of equipment, yet their functions differ.*

Keywords: *cybernetic and electromagnetic environment, automation*

Streszczenie: *Nowe technologie stały się czynnikami, który powodują, że od momentu ich powstania w środowiskach elektromagnetycznym i informacyjnym trwa cicha i intensywna wojna. Narzędziem prowadzenia tej wojny jest informacja przesyłana za pomocą sygnałów do wielu różnych odbiorców. Technologie wykreowały nowe środowiska działań. Środowisko cyberprzestrzeni jest tu przykładem sztucznie stworzonego środowiska walki. Staje się główną płaszczyzną przekazywania informacji w dowodzeniu, rozpoznaniu, walce elektronicznej, artylerii i wielu innych gałęziach działania wojsk. W referacie poruszane są kwestie związane z automatyzacją działania urządzeń elektronicznych pracujących w dwóch różnych środowiskach: informatycznym, (cybernetycznym) i elektromagnetycznym. Oba środowiska pracy zazębiają się i mogą wykorzystywać te same urządzenia, ale ich funkcje są różne.*

Słowa kluczowe: *środowisko cybernetyczne, elektroniczne, automatyzacja*

Gaining the upper hand and, in the long run, achieving victory is an aim that each of the battling parties strives at. Supremacy can be achieved through a variety of measures ranging from political pressures to military action. The rapid technological advancement of IT engineering has given rise to clandestine and intense war in the electromagnetic and IT environment. A signal transmitted simultaneously to a large number of receivers has become a tool to wage this kind of war. The signal itself is devoid of power and mass. However, when combined with the signal that transmits it, it becomes a decisive factor end stage of military action.

New technologies have given rise to new potential areas of warfare. Cyberspace is the most telling example of an artificially created environment in which bits transmitted through an appropriate signal play the dominant role. This new warfare environment has been claiming an ever larger proportion in the ways of sending and receiving information command, reconnaissance electronic war, among many others. An in-depth grasp of the functioning of electrical apparatuses in a new environment constitutes the gist of the paper at hand.

The article mentions topics closely connected with the automation of electrical devices operating under two different conditions: cybernetic and electromagnetic. One dovetails with the other and both could use the same type of equipment, yet their functions differ. The common area of operation of equipment in both environments and the possibility of their undergoing the process of automation allow whole new reconnaissance systems to be developed. Furthermore, the paper attempts to define the foregoing environments through the prism of operating in network-center environment. At the same time some effort will be made to point to a new meaning of the concept "work in an electronic environment" taking its source in information hostilities.

1. Introduction

Since the middle of the 20th century we have been observing a revolution in science and a rapid development of the industrial world is characterized by a vast production and consumption of a variety of goods manufactured by man and those used as crude resources. Not only have electronic devices dominated the life of man, but also industry in general, the lion share of which has been taken up by the military. Currently many scientists are of the opinion that Electronics and Informatics have become part and parcel of everyone's daily life.

Military engineering in WW II was developing fast, as seen from that time. Electronic equipment was very modern (electron lamps, triodes, pentodes), yet not without limitations, mainly power consumption and size. The first major breakthrough came with the scientific design and development of the magatron lamp used in radiodetectors. The revolution proper transpired with the close of WW II. The transistor and integrated circuits triggered a boom in electronic circuits of various use. The military sees in it a great potential and have put electronic devices to a wider use in such areas as communications, reconnaissance air defense, and artillery. Electronic equipment is used in military vehicles on more

regular basis (tanks, armored vehicles, wheeled vehicles, and modern stealth aircraft steered by man). Perhaps in not so distant a future similar aircraft following UAV (Unmanned Aerial Vehicle) will be carrying out military action.

Flying space is not the only one where electrical devices reign supreme. The navy with its warships and submarines is yet another example of metal leviathans packed full with missile steering equipment, command, recon, communication, electronic battle, unit control etc. Any one vessel is a self-contained stronghold. Be it alone or in a group of vessels, it is capable of locating, recognizing, destroying a target at a large distance. Warships are equipped with state-of-the-art technology, being a life example of how to forge cutting edge ideas into practicability.

Without electronic equipment and computerization space flight would remain unattainable. The recent mission of the last space shuttle *Atlantis* does not put paid to space exploration. It merely marks an end to a stage, in which Electronics and Informatics have dwarfed the obsolete technology. Needless to say, one must not disregard military engineering on land. *Steel stallions* are movable robots, in which electrical apparatus serves as basis of a well-aimed fire the targets sighted. The crew operates a vehicle enabling defeat of the opponent from a safe distance. Finally and most importantly, there is the man-soldier. The soldier of today may not be cyber-soldier yet; however, taking into account the sheer amount of electrical military gadgets at his disposal, one can go as far as to talk about revolution with respect to soldiers' add-ons. While personal firearms is still considered basis of any soldier's equipment, every so often one hears about PDA computer terminals enabling more efficient command, sending information hostile reconnaissance and aiming more efficient fire, at the same time staying clear out of sight. All of the afore-mentioned electronic devices remain operative in electronic, electromagnetic or IT environments. Each one separately or together with others, the devices can all be identified and jammed with electromagnetic energy or with a signal carrying a program that infects an operative system.

The problems seem to lie with the identification of devices working for electronic warfare systems on the one hand, and those that could be used in an information environment, on the other. As inanimate matter, electronic equipment, in general and its operativeness in particular can undergo automation.

Caution should be kept, as to which devices and in which order as well as to whose benefit can undergo this process. This paper is devoted to these particular issues. The first two chapters are concerned with the use of electronic equipment in an electromagnetic (environment) and cybernetic exploited in electronic warfare systems. The contents of those chapters exemplify the possibilities of identification of devices with a practical potential in both environments being the same apparatus but serving different functions.

2. Hostilities in Electronic Warfare Environment

Electromagnetic Waves as a Combat Environment

Until relatively recently the range of light visible to the naked eye was sole range of the spectrum used inadvertently by man. In battle the visible light spectrum was initially used to collect data through observation and to transmit a priori established light, smoke and similar signals. However, those ranges of the spectrum as well as subsequent means capable of transmission were considerably limited in the distance to which signals were relayed. Inevitably, transmission was dependent on the broadcasting position (Data Terminal Position) as well as particular transmission sectors. Not until the invention of discovery of radio waves was the electromagnetic space used to its full potential. Following this, the possibility of confrontation in this very environment materialized.

The last decade of the 19th century saw the a confrontation in the electromagnetic space. This was marked by the invention of the first wire telegraphs and transmitting militarily useful signals via radio waves. War, as seen from this perspective, began to take shape at the turn of the 20th century. It was at that time that a certain level of technology was reached allowing the radio to pay service to the military. Almost simultaneously, with this new use for the radio there was a sudden outbreak of war within the electromagnetic space. At the very beginning, military operations aimed at intercepting and deciphering information sent via the radio. Moreover, as a standard procedure they sent out signals in order to disrupt the ones sent by the enemy. With radiotechnology ever quickening its pace of development, new methods of waging clandestine war began to emerge. Novel solutions, based on divergent scientific thought began to emerge, these included: reconnaissance, pre-emptive strikes, radiolocation, and radio propaganda.

In the years separating the two World Wars the seeming gigantic radioelectronic advancement did not translate itself into new modes of combat nor into improvement in combat methodology. The main area of confrontation was reconnaissance and warmongering done via radio programs. This was mainly in the KF band. By contrast during the 2nd World War, following 1940, the opposing armies saw a rapid development in the forms and means of waging electromagnetic warfare.

The allied forces' scientists and engineers brought to a successful end a multitude of programs that provided the military with substantial quantity of modern reconnaissance and jamming equipment capable of efficient work across a variety of frequencies. Furthermore, this new technology could emit signals disrupting electromagnetic energy of considerable intensity.

The Third Reich and other Axis Powers were unceasingly carrying out developmental research. They were focusing acutely on defense reconnaissance and radiowave interferences. Through such steps they strived at maintaining the livability of their radioelectronic systems. The aftermath of World War Two was characterized by an intensive speeding up in the improvement of technology and

forms of waging electronic war. The whole process was further galvanized by experiences gained from different local wars and pockets of military conflicts. Especially relevant ones to the issue discussed here are the following: The Korean War of 1950s, The Vietnam War (1964 - 1973), The Middle East Conflicts (fought in the years 1967, 1973, 1981), The Battle of The Falklands (1982), The Persian Gulf War (1990 - 1991), The War in Yugoslavia (1999).

The aforementioned conflicts have all paved the way for the modern electromagnetic warfare. Operations carried out across FM waves have come to be dominant in the aerial, marine, and ultimately cosmic environment. This viewpoint is very clearly reflected in West European countries' policies and in their use of electromagnetic warfare systems.

The Iron Curtain countries of the Cold War period firmly believed that electronic appliances' primary function should rest with the Infantry. It played a secondary role when it came to the Navy, and Aircraft. The overall proportions of this technology being installed and their tactical usage are visible to this day. Such a glaring disparity of approaches to the same issue takes its source in World War Two experiences. It is also justifiable by scientific and technological boom in the Western Block. More importantly, one must not disregard here the ongoing arms race. Its main two sides The USA and The USSR were bent on worldwide domination and were in an urgent need of advanced reconnaissance systems that would remain operative over vast distances.

At that time it was only long range aircraft that could meet the high technical standards set for reconnaissance. Back then space reconnaissance was at its "drawing board" stage. US strategic reconnaissance gave rise to new directions on the development of electronic equipment, including recon and jamming devices. Long range reconnaissance with an accompanying spurious signal stands at the center of innovativeness. It constitutes the essence of technological thought and prevails in construction and later use of electronic devices. The electromagnetic wave setting has become undeniable domain in the arms race and covert operations.

The Work of Electronic Warfare Systems under Electromagnetic Conditions

In accordance with the established doctrinal provisions, operations taking place within electromagnetic setting are carried out in all manner of military activities and should be taken for granted. Such operations are mainly the domain of special units equipped with reconnaissance, jamming, and electronic defense systems. The electromagnetic setting allows for electronic warfare. Thus, the operative area of electronic warfare is electromagnetic space as well as radioelectronic sources emitting and receiving electromagnetic energy. The EW (electromagnetic warfare) setting is characterized by the following traits: the range of electromagnetic spectrum used, the density of frequencies used, the surrounding density of electromagnetic energy, the total number of operating electromagnetic devices per square kilometer, the deployment of individual radiomagnetic devices and their

proximity in relation to the contact line of troops, the specification and distribution of key military facilities e.g., main communication junctions, radar stations, reconnaissance centers, communication satellites. Electronic war spans over the same range of frequencies used by hostile radioelectronic systems which include communications, radiolocation, teledetection, and radionavigation. The relevant bands range from 30 KHz to 40 GHz to infrared and finally to light visible to human eye. The deployment of particular radioelectronic devices which areas and which frontiers are manned with the required amount of equipment. Being familiar with charts down to minutest detail is key in estimating the effectiveness of RM (radiomagnetic) interference from specific sources. Moreover, it is essential that there be a detailed specification of vital RE (radioelectronic) facilities as well as their viable positions. This is done in order to set a proper course of action for reconnaissance and allow appropriate amount of time for jamming with the use of electromagnetic impulse or munitions.

Electronic Warfare with diversified operational and tactical activities of its troops strives at gaining information about the systems and measures of electronic ground forces, the aircraft forces and its defense potential, the navy, weapons operating in outer space. Disruption and deliberate disorganization of reconnaissance systems of hostile armies and their commanding officers is central to its definition. Of all the mentioned ways of waging this kind of war, the EM waves setting is slowly but surely taking the lead. One can provide a number of examples of armament systems where electronic devices play a subsidiary role in achieving the expected results is of top priority:

- command and communications systems (C2W)
- radiotechnical systems
- munitions control systems (missiles, UAV)
- reconnaissance systems (e.g. optoelectronics)
- aircraft defense breaking systems (SEAD)
- electronic warfare systems (including EM impulses)
- IT systems (including cybernetic systems)
- navigation systems (GPS, Glonass)
- various back-up systems used by the navy and ground forces

The electronic equipment in question is being used continuously irrespective of war, crisis or peace. The only factor susceptible to change is the extent of military operations in each of the respective states.

The approach toward the work of electronic devices in EW environment within the Polish Armed Forces and in relation to the whole theory refers to specific tasks and is strictly task-oriented. During peace military headquarters make all the necessary preparations over a certain timespan. Those preparations are subsequently tested on the range. The planning officers of particular electronic combat units analyze hostile activity, assess potential risks, plan the chain of operation stages, see them through, and finally check whether the entire enterprise has yielded the expected results. They verify this by receiving the enemy's signals from particular

bandwidths. Should the operation turn out a success they proceed with the next stage. If the results do not come up to the expectations, the whole procedure is repeated or the final decision verified and the operation continues. The rule of thumb in operations and planning is: plan-realize-check-verify. It has a strong footing and immense historical background and has been widely used by virtually any armed forces involved in electronic warfare.

For almost eight years now a new concept concerning EW has been on NATO's agenda. Its centerpiece is to ascertain specified end results even prior to planners begin their work. The concept came to view in a publication issued in 2008 under the title, *NATO Electronic Warfare Policy* (MC 0064/10). It rests with the planner to define the results of electronic combat operations conducted under electromagnetic conditions. Moreover, it is their duty to assess how this will affect the success of the operation. This leads to an entirely new outlook on the planning phase, the preparation and the actual carrying out of electronic combat.

The previous approach had it that with a certain amount and specific type of EW equipment, the enemy's EW potential was expected to be diminished. What was taken into consideration was the degree of damage to hostile electronic potential with a rough estimate of the outcome of the battle. The operation was to be repeated until the desired effect. The latest approach, by contrast, is achieving the objective by any means. Depending on the challenge ahead a varying amount of equipment and munitions is used in order to accomplish the end result. If the EW arsenal of a given country happens to be insufficient, it is enhanced by a surplus from other NATO states. Thus the new framing of electronic warfare assumes joint operations. In a leap-frog over the next few subsections, it could be claimed that such operations will most certainly play a fundamental role in future electromagnetic warfare.

The Automation of Work of Electrical Equipment in Electronic warfare Systems

The concept of automation is applicable to both the analytical and planning process. Moreover, it also refers to the procedure of realizing combat operations via the electronic route. Finally, one can talk about the automation of information transfer to the decision-maker and back. A consequential question follows: can all processes be automated? ; And also, can all reconnaissance and jamming devices be coupled into separate automated systems? The latest generation of these technology items leaves the assembly-line semi- or fully automated and serve as multi-task appliances. We run up against problems trying to piece together the old with the cutting edge. Keeping to standards in this situation borders on the impossible. Some items fail to be automated due to their technological incompatibility. Others can be automated, however only to some extent. Financial and technical analyses state in no uncertain terms that building EW systems on older generation devices will generate financial losses. A more advisable solution would be the development of a whole new system based on our own engineering thought and with the aid of domestic industry. To better understand the problems

connected with automation, it is essential to possess a good knowledge of the characteristics of conducting operations in electromagnetic environment. Polish Armed Forces fight this war mainly from the ground and the sea. In other words, operations are run in a limited two-dimensional environment. Here we can talk about the width and depth of the battlefield zone. The potential role of the airspace has been underscored, but thus far severely underused. The possibility of realizing tasks has been diminished by tactical units demarcation lines as well as the limited range of communication between them. The pervasiveness of EW combat can be impeded by the inability to receive electromagnetic emission i.e. the radio horizon for VHF, UHF, SHF, EFH bands. Also, of much relevance here is the distribution of hostile electrical equipment. The total number of EW systems at the Polish Armed Forces' disposal leaves much to be desired. Currently, we are far from possessing a full-fledged automated EW system. Not even the automated system *Wolczenica* can render the military fully automated. It is still the case that many subunits fight with no automation whatsoever when it comes to tactics and operation. The whole of reconnaissance and jamming is done manually through soundwaves from command post subunits. This leaves the commanding officer of the subunit with insufficient time for reaction to the rapidly changing conditions on the battlefield. Combat dynamics is characterized by a quick pace of change. Consequently, without an instantaneous reaction to the detected sources, the tactical unit will be exposed to electronic hostilities from the enemy. In practice, there is no need to jam every single source. In some situations it is left to the soldier's discretion to decide which source should take priority. That is why automated commanding and controlling apparatus should be equipped with a manually operating equivalent.

Fig. 1 Company EW formation at the tactical level

The tactical operating of a company EW via the radio is by direct orders issued by G2 SD tactical unit (Fig. 1). The entire system is controlled by EW chief commander and individual posts are run by company EW commanding officer. The update on the progress of the operation is sent to the analysis and assessment team in the G2 unit. The presented command mode of the company EW unit devoid of a fast radio connection severely undermines the effectiveness of electromagnetic combat. This is also the case at the operation level. Without automated systems, the HF band cannot be used to its full potential. A particular subunit equipped with outdated technology does not match the high standards of the modern battlefield. The lack of automated systems controlling reconnaissance and jamming has its consequences in the located radio signal being terminated even before the jamming initiates. The HF jamming subunit works in phonic-manual mode most of the time, although it also has an in-built semi-automated control unit. Its wear and tear causes its fallibility. The EW system code-named *Przebiśnięg* was to have been an answer to these shortcomings. The system is used by an EW company at the level of tactics. It constitutes an internally automated system at the subunit level. It has significantly improved the system's detection, tracking, and jamming capabilities. Up to now, it has not reached the required reconnaissance penetration across the entire reconnaissance zone of the tactical unit, approximately 50 km., even though the antenna was operating at 50 meters above sea level. Each subunit in the system is controlled via radio using TDMA time loop emitted from the commanding vehicle. This is synonymous with automation. What is more, each system is perfectly capable of individual work, being independent from others, and aggregating information intercepted by the commanding vehicle.

However, one downside of the system is the yet unresolved problem of simultaneous display of the results obtained from reconnaissance and tracking in the company EW commanding vehicle. The commanding officer has only radio or radiolocation devices to rely on. He or she does not have insight into data verification essential in assessing the tactical and/or operational character of each source. Yet, the very basic design flow of the *Przebiśnięg* system is the lack of direct connection of automatic data transmission and control in the commanding tactical unit. The commanding unit should be able to send and receive data to and from the system respectively. It is a top priority that this missing element be designed, developed, and put to use in the ground forces. It is vital that a vehicle receiving and sending data automatically should be able to make use of the existing means of transmission. Otherwise the system will co-operate with EW subunit only. If this is the case neither the commanding officer nor the headquarters will receive data in real time but with a considerable timelag. There is a real danger that vital decisions will be taken based on partial data. This being said, it is obvious that automation of EW subunits is an absolute necessity.

In the future development of EW systems main emphasis will be placed on data transmission. The speed with which reconnaissance and prevention function have a

major say in the efficiency of the systems. A fast track to achieving this goal is possessing a perfect medium of data transmission. Still in the pipeline, the system *Kaktus* is to meet this requirement. It will be able to transmit data in almost real time. The system, apart from having an internal automated module, will be equipped with external modules as well. With a variety of communication systems data aberration will hardly be noticed. Such technical solution ensures unhindered flow of information in the form of written text, graphics or images. The messages will be able to carry substantial byte-load and will not lose out on quality. For the operation to be carried out in sync with the commanding unit an appropriate reception model is a prerequisite. A separate transmitting vehicle with a direct access to the internal system of data circulation should also meet this condition. Without one even the best system remains a manually operated device of a very limited use. In this type of units, data have to be collected first, then processed, and finally presented to the commander, who is the ultimate decision-maker. Needless to say, it takes a considerable amount of time for the data to end the full cycle.

Currently, EW units in the Polish Army have a large portion of this technology produced abroad. The technology is being used at different frequency bands. The vast majority serves to identify and track radio sources. The search and interception of signals relevant for EW units is central to reconnaissance proceedings. The technology used today is capable of detecting most signals, the medium being electromagnetic waves at virtually all frequency bands. The intercepted signals are not always broadcast by radiotransmitters. Oftentimes the source of transmission cannot be established with certainty. The spectral analysis of such signals helps conclude that their origin may as well be radiowaves, computer emission or microwaves. Signals of this type will also be detected and intercepted. Going back to the *Przebiśnięg* system again, it must be pointed out that there is a possibility to detect and track electronic devices that are beyond the interest of military decision-makers. Radioreceivers are designed to receive signal up to 3GHz and radiolocation receivers up to 18 GHz. The problem lies in their ability to identify signals. With an appropriate database built up of signals carrying no information at all such identification is possible. Therefore, reconnaissance appliances can serve a double function. Some will satisfy the needs of EW, others can be used as multifunctional recon apparatus, depending on the need and applicability. Apart from EW purposes, multifunctional receivers will be searching for atypical signals at different bandwidths. With available database patterns serving a touchstone function, it will be possible to identify and jam the source of emission. Here the jamming procedure is a whole different issue in itself. Jamming devices emit energy that makes hostile devices dysfunctional. The information thus transmitted changes its character, and in other situations it is destroyed. The role of those devices is twofold as well. They may be used in EW systems. They may also be used as signals distorting the signal proper in computer networks. If it is assumed that spurious signals carry an additional program such as a virus, then this kind of

hostility lies in the domain of cybernetic environment and can be dubbed cybernetic warfare.

3. The Cybernetic Environment – Terminology

Operations across and within computer networks should be understood through the prism of the changes that have been taking place in times of military conflicts as well as operations other than war. With the end of the Cold War period and global, bipolar military status quo, an entirely new political situation has emerged. The situation has changed dramatically when it comes to global security. Over the last few decades we have been witnessing emergency situations we never faced before. An immediate result of those changes is a non-standard use of armed forces and a new approach toward planning, commanding, controlling, and collaborating with domestic troops as well as allied forces abroad. We are also observing a major change in the attitudes toward non-military organizations, for instance, humanitarian organization under military supervision. The massive influence those changes have, has given rise to a number of asymmetric effects on domestic and hostile forces. This exemplifies new hazards in the area of military operations. The traditional methods of waging war are being superseded by surprise attacks in small groups of troops in many places simultaneously. A physical attack, aside from gunfire, has come to be associated with other mediums and cyberattack certainly counts as one of them.

Cyberspace is the “primordial soup” that spawned all manner of means of information transfer be it the spoken word, printed messages or images at present, and holographic images in the future. As far as easy availability of information is concerned, global data transfer constitutes a bona-fide revolution. The military are trying to make the most of this state of affairs. Any commanding officer’s decision can be tracked online. Commanders and their troops have become mass media hostages. Their decisions are assessed by domestic and foreign audience. The cybernetic setting, which has become their working ambience, is transparent to the public opinion always hankering after the latest developments.

The fast tempo of development in the IT area made such easy access to information possible. Countries all over the globe started coming up with different definitions of information networks. The concept as we know it began to take on new meaning when approached from a global perspective. It has been extended to encapsulate gathering data, detecting and jamming the information setting. For some time there has been a noticeable increase in the bulk of material published on the topic of cyberspace. Many authors have been taking the term for granted, without giving much thought to its true meaning. Some of them seem to blur and skew its meaning in attempting to present their views. One consequence of the nascent change was a new doctrine proposed by the US Armed Forces in December 2008. It was made public as *The National Military Strategy for Cyberspace Operations* (NMS-CO). It defines the cybernetic domain, enumerates potential threats, and nephralgic areas. It constitutes a basis or further military action in this area. The

doctrine itself is an expression of a multidimensional strategic approach by US Army to the use of cybernetic operations ensuring the nation's supremacy in this field. According to the doctrine, this objective is to be achieved through integrated cybernetic offence with defensive operations aided by highly-qualified personnel. The doctrine is an attempt at defining cyberspace.

Cyberspace is a domain characterized by the use of electronics and electromagnetic spectrum for gathering, modifying, and exchanging data via network systems and accompanying physical infrastructure. The document contains an older definition from a previous publication (JP 1-02). It reads as follows: cyberspace – a virtual environment in which digitalized information is made available via computer networks.

These two framings of cyberspace differ glaringly when juxtaposed. While in the older version access to data is exclusively through computer networks, the latest version includes a selection of electronic devices and accompanying physical infrastructure. Both definitions refer to already existing information networks. However, cyberspace's social dimension should also be taken into account. The tradition social relations stand in great contrast to the ones maintained over and with the help of the Internet. Time and space lose their core meaning in cyberspace. Interpersonal relations are of the essence. In this respect borders between countries have ceased to exist and people using the Web have become uncontrollable. Everyone is connected to everyone else while remaining an anonymous netizen.

It should be reiterated that cyberspace can be approached from different angles. It could be treated as human activity aided by information technology, where all activity is synonymous with technology, and where geographical notions are irrelevant. As was pointed out by P. Villo "... its elements are devoid of an expansiveness dimension, they function within and can be subsumed under a specific timeframe across which information flows. [...] Integrated computers and computer displays render the division into the *here* and *there* non-existent.

It is almost a cliché to say that cyberspace is a new medium transferring data with lightspeed by means of bits. Even without a sharpened definition we seem to know instantly that what authors have in mind are computer networks in general and the Internet in particular. Cyberspace is treated as something created artificially. A value stripped off geographic parameters, immensurable and limitless. As Z. Bauman pointedly observed: "its frames and boundaries are measured by the current level of IT advancement and the extent to which the world has been Interneticized". Indeed, what we call distance in cyberspace is far from being an objective impersonal datum physical in character. All remaining factors, by means of which group identities arise, gain and preserve their uniqueness.

The character of contact between networking users has changed since the first stages of cyberspace. Interpersonal relations have turned into a form of a partnership, while the freedom of speech is gaining wider and wider ground. Territorialism has become a thing of the past. It is no longer possible to control who communicates what to whom. The most pressing issue then is not so much an

unimpeded flow of information but control of virtual space. Democratic countries wanting control cyberspace are obliged to adhere to the fundamental human right, the freedom of expression being one of them. It has been decided that since cyberspace cannot be controlled, the effects of its functioning ought to be minimized.

The results of those measures can be observed in a limited access to some Internet content granted to its underage users. Access to sites promoting pornography and violence are automatically censored. Similar steps are taken by companies toward their employees. The same is the case with authorities banning access to aggressive, subversive or otherwise unwanted Internet content. In some Asia and Arabic such practice has become standard. Many authoritarian regimes go to great lengths to keep their society ignorant. They purposefully block Internet sites, some of which are fertile ground for insurgency. Such countermeasures may prove effective, as a broadband connection in these countries is still a rarity.

Cyberspace is thoroughly discussed in an official document published in Poland in 2008 titled *Governmental Program for Cyberspace Protection for the years 2009-2011 – Provisions*. It is a reaction to different measures taken by EU. The document provides specific guidelines for the Polish presence in cyberspace. It also provides a simple definition of the term, which reads: *Cyberspace is communication space consisting of a system of internet links*. It provides some names of governmental organizations working in cyberspace environment, which include: MSWiA, ABW, MON, SKW. Moreover, it mentions non-governmental organizations, owners of resources, etc. It informs that the Polish MON has been granted its own share of responsibility for cyberspace. The legal basis for the Armed Forces jurisdiction is the document *Decision of MON nr. 375/MON dated 29/07/2008 concerning the response to computer incidents in the National Defense Department*. This can be taken as read that the military had already been involved in cyberspace activities.

Following government decisions The Minister of National Defense formed The Polish Armed Forces Center for Cybernetic Security, which is to be in charge of cybernetic hostilities at the operation level. Professionals working at the office define operations in cyberspace as an easy access to and wide use of electromagnetic waves. Following their idea of cybernetic activity; *It is a global expanse within IT setting comprising the Internet, telecommunications networks, IT systems. Cyberspace can be understood as accomplishing different objectives via cyberspace route. Those measures include activities whose aim is to gain and protect relevant data*. This take on the matter corresponds with the American definition. Cybernetic operations are a true evolutionary milestone. Obviously, the trend setting country in this respect is The United States. It can boast of the most advanced IT in the world. With the document DD 3 – The US tries to define cyberspace extending its core meaning by cybernetic operations and cybernetic defense.

The concept has been extended to include by an IT domain. Here, cyberops are explained away as cybernetic solutions where self-interest plays key role. Such operations include activities in IT networks and activities defending Global Information Grid. The set of aforementioned definitions help to sharpen the concept of cybernetic advantage to operating in cyberspace as a method of carrying out hostilities in a given time and domain without unwanted interference.

4. The Correlation of Electrical Apparatus

After WW2 both civil and military theoretician were of the view that future wars will be strictly tied with outerspace and the electromagnetic spectrum. The views expresses placed the EW waves as the most palpable background for military conflict. This claim is substantiated by numerous examples of the use of electronic weapons throughout history. The evidence for the shift toward EM dimension is further confirmed by many innovations introduced to the field over the years. The view expressed by the historian Michael Howard in his book *War in the History of Europe* tellingly frames the issues related to the development and use of electronic means of communication, cryptography, reconnaissance, and radiolocation. (...) *The side that prevailed eventually was more capable of keeping track of the enemy's movements, deciphering its messages, and at the same time it could keep its own secrets secret. During World War Two this would not have been possible without the know-how of intercepting radio signals.*

It can be assumed that already in those years a new war environment was being exploited. One can bring forward countless examples of attempts at categorizing military activities and defining all war dimensions.

Up until recently military confrontation was taking place in a three-dimensional environment. This matches very closely human cognition and understanding. Strife at a modern battlefield transcends these barriers. Some theorist talk about as many as six modern warfare dimensions altogether. One of them is colonel R. Grabau of the German Armed Forces who discusses the multidimensionality of war by pointing to six aspect in waging it. The first three are rather standard and include the following: X-width, Z-depth, and H-height. Additionally, he introduces time, information, and electromagnetic spectrum. He envisages the last three factors to be decisive in future conflicts.

The same conclusion was reached independently by a colonel from United States Airforce in the first years of the 1990s. Colonel John Warder put forward his claim of strategic paralyze, where he presented his Warden's Model. According to his theory, any enemy can be seen as a collective system of subsystems. Thus, any organization can be regarded as a structure composed of five inner rings that form a unit and serve different functions. He includes in his model a number of organizations: companies, the military, terrorist organizations, organized crime, among others. Here is an approximation of how his model is supposed to work:

- Political elites i.e. the controlling factor.
- Basic institutions – earlier referred to as organic needs transferring energy from one ring to another.
- Infrastructure.
- Society – the human factor.
- Defense Systems – composed of demographic groups.

The model is organized along the following lines; each of Warden's rings functions in a specific setting: the sea, ground, air, cosmos, cyberspace. Taking into account current conditions, the model asks for a slight modernization. Nowadays the preferred setting for various activities is electronic rather than electromagnetic. Thus the fifth ring is divided into two parts, the cybernetic setting and the electromagnetic setting.

Fig. 2 A modified version of Warden's Model
Source: Own work

The problems with automation of electronic devices concern the EW waves environment. Neither automation nor electronic systems are keenly pursued issues by the Polish military decision-makers. The past as well as ongoing military conflicts especially in Bosnia, Iraq, and Afghanistan provide irrefutable evidence that the IT setting is getting importance almost by the battle. Hence the questions: Can electronic equipment be used to detect IT networks? If that is the case, then which devices are these specifically? Can these devices also work in other environments? Perhaps they are operating within a yet undefined one.

Traditionally a battlefield used to be described as an closed geographical area, within which hostilities are carried out. The very definition of the battle field imposed ways of waging war. Nowadays modern combat uses other environments as well. By their nature, they are far removed from the battlefield in geographical sense, which is responsible for the radical change in the ways war is waged. This is noticeable even at the very fundamental level. As a case in point may serve network-centric hostilities connected with maintaining a continuous, unimpeded flow of information from the decision-maker to appropriate sensors. Multifunctional devices of global range help individual troops accomplish strategic goals. They keep soldiers up-dated by continuous flow of data so that they can take optimal decisions. Another telling example is antiterrorist hostilities, especially the ones in a network-centric environment. In the case of opposing an unidentified enemy it is difficult to talk about battlefield as such. In this context military operations rarely bring the expected result. Asymmetrical conflicts are characterized by atypical battlespace area. The enemy and its pursuer are constantly on the move. The side whose position is compromised loses out. Conversely, the side fighting by stealth controls the situation.

A reaction to this state of affairs was a new concept propose by the US military. What was used to be called battlefield is now superseded by battlespace. It includes strategic, operational and tactical conditions irrespective of their geographical location. From this angle, operations even at the tactical level are conditioned by a vast number of factors, most of which lie beyond the commonly understood *battlefield*. Here, one can talk about other settings for activities. Generally speaking, traditionally organized operations limit the maneuverability of the commanding officer with respect to monitoring and assessment of the situation. His recon capacity is not fully used. This situation is instantly mended with the application of a network centric approach toward military operations. In other words, the IT and electromagnetic environments prevail.

The use of electromagnetic energy in air, cosmos, and water, as well as the use of computer systems in cyberspace directed military action toward a totally new environment where Electronics plays the most important role. Obviously, arms in the traditional understanding will long remain a vital part of any army's arsenal. However, they will probably be used to scare off potential enemies. The common denominator for this environment are electronic systems and devices. We have thus entered a new era of electronic environment. One cannot overvalue its role as it is used to operate and control virtually every piece of equipment. Man is an essential component of this mechanism. Autonomous military operations are now possible, which is another great achievement in the field of cybernetic science. Independent operations carried out at sea, in the air or on land with the use of electronic equipment further bear out the claim that we are witnessing the emergence of a novel battlefield environment.

Fig. 3 The working environment of electrical devices in Electronic Warfare and Network-Centric Setting.
Source: Own work

With this in mind, the electronic environment can be described as follows:

- The set of all objects including their attributes and dependencies between them, which due to certain criteria of assignment to the system, have been excluded from it.
- The totality of inanimate elements both natural and created by man existing within a particular area including the links and dependencies between them.

The concept of the setting in which electronic devices function has been narrowed down to the total number of inanimate elements resulting from human activities in particular time and space.

The paper at hand has viewed the electromagnetic setting from many different angles. A considerable amount of space has also been devoted to a number of problems connected with automation of electrical devices in their working environment. A different issue is automation in other environments. The resultant question is, can equipment be functioning in other settings be also automated. The characteristics of the setting have been provided. The conclusion is that electrical devices functioning in this setting are mainly computers. However, apart from them, there is a wide range of auxiliary appliances.

Carrying out operations in cyberspace means facing the same challenges pertaining to Electronic Warfare. The hostilities in both environments are comparable if one

assumes that the means of combat in cyberspace are reconnaissance, jamming, and defense. The fundamental question is whether they are the same in nature. Cybernetic reconnaissance aims at gaining information about the movement of objects in computer networks. In other words, it is concerned with gathering data that is of interest to the recipient, intercepting information from identified objects, detecting relevant sources and tracking them. Therefore, it can be concluded that these are very similar tasks that lie at the core of Electronic Warfare. What has partially changed are the tools used to accomplish these goals. The radioreceiver has given way to the computer equipped with appropriate software. This software constitutes the key and the fundamental difference between cybernetic and electromagnetic warfare. With a closer look at the issue one encounters a further problem. Computers are equipped with receiver-transmitter devices such as Wi-Fi or Bluetooth. Consequently, an electronic appliance together with a computer form a transmitter-receiver system. Through their protocols, Wi-Fi devices allow for the data to be transmitted over a long distance by means of 2.4 GHz electromagnetic waves. Taking this into consideration we can say that receiving devices are starting to function like similar devices used in EW. In a nutshell, information reconnaissance is electronic reconnaissance realizing of searching emission sources, intercepting and tracking signals transmitted via electromagnetic waves. What changes is the character of the detected devices. By contrast, information reconnaissance within cybernetic warfare focuses on the search for objects, programs, their interception, detection and tracking in computer networks with the use of impulses and, to some extent, electromagnetic waves. The way to access computer networks is via electromagnetic spectrum or direct connection to the network.

Fig. 4 The idea of radioelectronic reconnaissance
Source: Own work

Fig. 5 The idea of cybernetic reconnaissance

Source: Own work

Granting that that under certain conditions radioelectric and information reconnaissance is feasible by means of electromagnetic waves, one may wonder whether it would be possible to construct a universal tracking device. Such hypothesized item would be able to monitor computer networks and other electronic equipment working at similar frequencies for both cybernetic and electromagnetic warfare. If we assume that EW breaks out in a civic setting then construction of the device is viable. With just one such remotely splayed item capable of receiving wide frequency spectrum, it would be possible to gain access to electronic devices being of interest to EW and to receive impulses at the working frequency of practically any network. Remote connection to such equipment will make it possible to connect to any particular network undetected.

Fig. 6 An model of a common locating device in electronic and cybernetic warfare

Source: Own work

Apart from electronic devices typical for electronic warfare, cybernetic warfare will also be using jamming devices and technology for cybernetic defense. Interference and jamming in this sense is tantamount to introducing spying software into computer networks. This means gaining specific data in specific networks and computers using all manner of methods. Moreover, what is also understood by jamming is introducing software in order to cause physical damage to software e.g., destruction of database content, virus infection, overload causing hardware to go haywire, deliberate overloading of the CPU, RAM, and graphics board. Broadly speaking, there are two ways of accessing computer networks. Breaking into computers from any place on the globe. The other being direct connection to network. Many receivers take necessary safety precautions, which prevents access to their databases. Information seekers are expected to possess a formidable body of knowledge, which with the level of IT education available, is not a problem at all. Additionally, a much more severe problem pose networks located outside the reach of cyberwarriors. Providing special units with universal devices might be a solution to this problem. Such devices could be used for electronic reconnaissance in the traditional sense, but at the same time they could monitor a given area for networks of interest. As soon as one has been located, the use of appropriate software, cybernetic warfare ensues.

Automation and universality of reconnaissance have been mainly due to costs cuts and tightening of the budget. Another consequence is miniaturization of devices and gear. The smaller a device is, the less it costs to produce. Best fit this role are sensory devices, whose functions range from detecting to jamming to booby traps.

Another issue is computer network security. From the point of view of cybernetic warfare, defense comes down to technical protection of computers with the help of programs, monitoring devices, surveillance systems. Furthermore, it includes barring access of unwanted individuals and/or programs to the network itself, the server, identification cards, and finally to the premises.

The automation of electrical devices for the needs of both EW and CW is possible to a certain extent and in relation to highly specialized reconnaissance devices. Experience gained from past military conflicts teaches us that future combat environment will force us to change much in our idea and attitudes. The proposals made in this paper may contribute to finding novel technical solutions.

5. Conclusion

The ongoing evolution in the organization of military operations in environments other than electromagnetic as well as permanent reorganization of reconnaissance does not concern strictly structural and doctrinal changes. Focus on other environments means a deep transformation, which is predicted to last relatively long, perhaps even more than twenty years. The heart of the matter is the a change in the mentality and concepts concerning with activities in IT networks and approaching electronic devices from a broader perspective. The electronic and cybernetic dimension is becoming reality. Personal, tactical, structural and

technological changes impress upon us different attitude toward functional and constructional considerations of electronic devices operating within different environments. Homogenous devices operation within a single setting are costly, inordinate in size, and easily detectable on the battlefield. By contrast, miniaturized multifunctional devices will be able to achieve levels of efficiency unattainable for older technology. They will excel at accomplishing complex tasks. Thus, automation of such devices is a prerequisite and a necessity.

These changes are being made and probably will be taking place during missions organized by the military. This is taken to mean that altogether three process are taking place in parallel: (1) the participation of reconnaissance in missions with the use of state-of-the-art recon gear, (2) automation systems, (3) the search for new technological solutions. That is why reconnaissance operations will be carried out under very hard conditions. Taking this into consideration, it can be assumed that in the coming years the dominant environment for The Polish Armed Forces will be the electromagnetic environment. The automation of systems will be developed systematically. When it comes to the cybernetic environment, the automation of devices is limited in range. Yet, considering the difficulties accessing certain networks, especially LAN networks, common electrical devices (sensors) could undergo this process.

New concepts referring to electronic equipment are discussed by different panels of experts. It is for academics to decide whether some will enter the technical language. After verification from scientific circles they will be included in doctrines and books. Those considerations are still to come.

Automation and miniaturization are changing scientists' views on problems of reconnaissance in different environments. Not only do the EW units work in EM spectrum, but they are also looking for ways to expand and work efficiently in other environments. With hindsight, the rapid development of technology and the speed of changes will cause a revolutionary shift from electromagnetic spectrum to a wholly new environment. It barely needs pointing out that we must do all there is within our power not to miss it and keep abreast with the times

6. Literature:

- [1] Bauman Z., *Globalizacja, czyli komu globalizacja, a komu lokalizacja*, "Studia socjologiczne", nr 3, 1997.
- [2] Bauman Z., *Globalizacja*, Warszawa 2000.
- [3] Bógdał-Brzeńska A., Gawrycki M. F., *Cyberterrorizm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, ASPRA-JR, Warszawa 2003.
- [4] Czeszejko S. *Działania elektroniczne w NATO i Siłach Zbrojnych Rzeczypospolitej Polskiej – próba kategoryzacji*, AON, Warszawa 2011
- [5] *Cyberspace Operations (DD 3-12)*, Centrum Rozwoju Doktryn i Edukacji Sił Powietrznych USA, 2010.
- [6] Grabau, *Sześć wymiarów wojny*, WPZ nr 1,2,3, Warszawa, 1987
- [7] Howard M., *Wojna w dziejach Europy*, Ossolineum, Wrocław 1990.

- [8] Konopka L., *Walka sieciocentryczne sposobem działania sił zbrojnych w przyszłości*, Myśl Wojskowa, nr 2/2006.
- [9] *Mały słownik Cybernetyczny*, Wiedza Powszechna, Warszawa 1973.
- [10] Materiały robocze Centrum Bezpieczeństwa Cybernetycznego, Białobrzegi, 2011.
- [11] *National Military Strategy for Cyberspace Operations – NMS-CO*, Joint Chiefs of Staff, Waszyngton, 2006,
- [12] Price A., *Narzędzia mroku*, Wydawnictwo Dolnośląskie, Wrocław 2006
- [13] *Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011 – założenia*, Warszawa, 2009.
- [14] Scheffs W., *Walka elektroniczna w operacji i walce*, AON, Warszawa 2005.
- [15] Scheffs W., *Środowisko działania sensorów walki elektronicznej*, ZN AON nr 4/2010
- [16] Sienkiewicz P., *Wizje i modele wojny informacyjnej*. w: *Spółeczeństwo informacyjne – wizja czy rzeczywistość ?*, Biblioteka Główna Akademii Górniczo-Hutniczej, Kraków 2003.
- [17] Vego M., *Systemowe kontra klasyczne podejście do działań bojowych*, Kwartalnik Bellona nr 2, Warszawa, 2009.
- [18] <http://en.wikipedia.org/cybrprzestrzeń>

plk dr inż. Waldemar Scheffs, adiunkt – Kierownik Zakładu Rozpoznani i Walki Elektronicznej Akademii Obrony Narodowej. Absolwent Wyższej Oficerskiej Szkoły Radiotechnicznej w Jeleniej Górze oraz Akademii Obrony Narodowej w Warszawie. W latach 1985-1993 pełnił służbę na różnych stanowiskach w pułku rozpoznania radioelektronicznego, od 1994r. jest nauczycielem w AON. W 2001 roku obronił rozprawę doktorską w specjalności dowodzenie. Autor podręczników i artykułów z rozpoznania, walki elektronicznej i działań informacyjnych.