Network Enabled Capability and the Impact on Education

PETR STODOLA
Department of Automated Command Systems and Informatics
University of Defence
Kounicova 65, Brno
CZECH REPUBLIC
http://k269.unob.cz/~pierre/

Abstract: Network Enabled Capability is being defined as a programme to enhance military capability by better exploitation of information. The paper deals with education and training of military professionals for the Information War. Correct and effective exploitation of information is found to be a crucial factor in this new form of war. Distance learning and e-Learning is considerable possibility for gathering and effective exploitation of information. The paper analyses possibilities and forms of wide-spectrum education and training which is necessary when considering construction complexity and ways the monitoring devices are being used. Individual areas of education and training are discussed. Although these types of education are not common in armed forces yet, recent development of digital technologies will require it.

Key-Words: Information War, Education, Training, Sensors, Monitoring devices, Diagnostics, Communication

1 Information War

The Information War (IW) is a new form of fighting at the dawn of the new millennium. Information is becoming the most powerful weapon of the new era. The effectiveness of weapon systems is directly dependent on the quality, trustworthiness, and timeliness of information about the enemy.

The IW is conducted in the sphere of information. If it breaks out in its full strength, the results are nothing less than surprising. It influences the drop in morale and fighting spirit of soldiers and in its consequences it has direct influence on the fight-worthiness of the army as a whole. The foremost specialists in this sphere are searching for still more effective modes of this form of war.

Based on experiences from armed conflicts in which the elements of the IW were used, the experts reached the opinion that the IW, if it is properly and skillfully conducted, can reach extraordinary successes even without the use of classic weapons and most significantly without the loss of human lives.

The term IW is quite wide. In it can be included activities in the sphere of communication, penetrating computer network systems, entries into data networks and their disruption or entries into systems of commanding the armies.

All the possible ways and forms of the IW are not known so far. As opposed to other and known kinds of war, it is difficult to recognize the start of partial preparatory activities and the offensive, determine exactly its breadth and analyze the elements of the information systems which have been attacked, and the form of attack, enumerate losses etc.

Attacking a part of a large information system that, at first glance, is quite insignificant, can cause a chain reaction, the consequence of which may be catastrophic. Therefore, education and training in an effective attack, but also defence, requires significant attention. Only exceptional expertise of the crews and operators will guarantee effective conduct of the fight.

1.1 Use of modern devices

Changing very quickly is the way the armies are being commanded. The contemporary battleground is filled with electronic devices and the area is saturated with signals of all kinds and frequencies. Electronic devices are supposed to support commanders in their decision-making and increase effectiveness of weapons. Commanders are quickly getting used to the digital battleground because they quickly convince themselves, in practical use, how complete an overview they have of the situation in the area of interest, which is many kilometers distant. The situation, therefore, becomes critical when commanders are deprived of the possibility of distance-commanding.

In general, it is true that the key factor of modern management of the fighting activities rests with the capability to collect, process, decipher and utilize

information about armed forces of the enemy, together with depriving the enemy of the possibility to obtain information about one's own forces, and the measures taken.

The basic prerequisite for victory in the IW is equipping the units with the corresponding equipment, which will make possible transmission, reception and display of digital information. Data networks, which are being built with intensity, installed in all the modern armies, will facilitate a very quick acquisition, sorting and distribution of relevant data about the battleground - the activities that are far beyond the ordinary human capabilities. High performance of the systems and equipment facilitates automatization of many routine processes.

Perfection, however, usually also means complexity. And the more complex the technical equipment, the smaller the possibility of a human being to control the functions taking place inside the equipment. Built-in diagnostic circuits which are, nowadays, already a given in most electronic devices can recognize the faults and deviations from the operational values, but usually cannot handle skilled manipulation of the data at the input or output.

1.2 Main weapons of the IW

The main weapons in the IW are the information means and technologies, which are used for fast and concealed manipulation of the military and civilian information systems of the enemy. The goal is to disrupt the enemy's activities, or make them impossible, and to conduct manipulations of the contents and form of the transmitted information.

It is supposed that the IW could be carried out both independently, without the use of the ordinary warfare weaponry means and ways of the armed struggle, and just as in coordination with them, in close harmony with other kinds and ways of fighting activities.

The IW is not oriented towards material, but towards information and data objects (that is, all construction elements of information networks, means of data transmission, computers, including all kinds of carriers of information). Measures taken do not have to lead to direct physical destruction of the enemy's material base, personnel and technology.

The possibilities and effectiveness of the IW are ever increasing, with the growth of complexity, operational possibilities and increasing the use of microprocessors, as parts of complex weapon systems and sensors. These can, in the hands of specialists, become a highly effective and powerful weapon, the real battle strength and possibilities of

which are, in its full breadth, possible to imagine only with difficulty.

2 Education and training

The presented facts and the properties of the IW must necessarily reflect in military education and training of persons who participate in war. Education and training must concern not only soldiers, but also civilian personnel.

It is in particular in the IW that the civilian sphere is participating more than in any other form of war. Especially in the development of effective methods and means of conducting the IW is where the civilian experts can participate.

Considering the great technological developments, it is obvious that it is necessary to periodically repeat education and training. Despite the fact that several armed conflicts, in which elements of the IW were successfully included, have already taken place, this form of struggle is still in its infancy. New possibilities, principles and technologies of the IW, with which it is important to familiarize both the military and civilian personnel, are continuously emerging.

It is, indisputably, necessary for everybody who is participating in war to be able to, as effectively as possible, utilize the possibilities of the IW, but also quickly and without errors react to possible actions of the enemy. A part of the training of both, individuals and units must, therefore, be not only the correct knowledge of how to use the variety of equipment and instruments, but also a flexible and cold-blooded reaction to their errors and dysfunction, which will be caused, by his action, by the enemy.

The time interval between the individual educational activities, and their form, depend on many factors. An important role is played by the function and role of the person being educated, that is, the measure in which he participates in war. Because there are many forms of the IW (and, in addition, the concrete contents and the external manifestation of the IW are not always completely discernible and, therefore, all possible means and forms are not fully known), the forms and means of educating the personnel also cannot be simply determined and assembled. The following text will, at least, attempt to emphasize some basic fields of education and training, which are the condition for successfully conducting the Information War.

2.1 Education

The figure 1 captures some of the basic areas of education of individuals and military units. The emphasis is on the understanding of physical principles and principles of functioning of the sensors and means of communication.
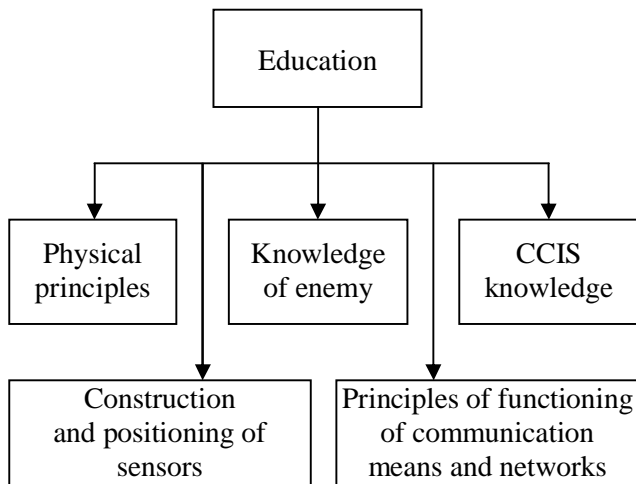

Fig.1 Education areas for the Information War

The first important part of training must be understanding of basic physical principles related to radiation, reception and evaluation of various kinds of energy in various spectral ranges for the interested entities. The operator must be conscious of all the possibilities of the instrument or installation, with which he is working. He must also be familiar with all the possible detrimental situations, which may occur as a result of the action of the enemy, and must react to them with flexibility.

Understanding the physical principles, which are used as tools for conducting the IW, is simply indispensable for effective control of the instruments and installations, and their use against the enemy and, conversely, for preventing the similar activity of the enemy.

The most important part of education in the field of physical principles is collecting and evaluation of various kinds of energy in various spectral ranges. The correct procedure during the collection and the following evaluation of the results makes possible determining the activity of the enemy in the framework of the IW. Individuals must be well familiarized with instruments and installations that collect the energy and signals. Even more important is to correctly evaluate the results of the collection. This area in particular has high demands on education of individuals.

The next important sphere in education of individuals and units are the ways of construction,

use and allocating of suitable sensors. Sensors are the main source of information, and, therefore, this part of education must be given extra attention. The figure 2 shows, with more clarity, the most important areas of training in the field of sensors.
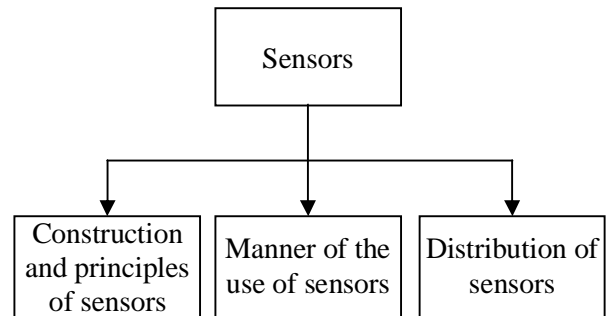

Fig.2 Education in sensors area

Selection of the suitable sensor is a basic prerequisite for monitoring and analysis of the area of interest. The correct selection of a sensor requires education of the individuals on a high level. The first step for this form of education is understanding physical principles and construction of various kinds of sensors. This is a strictly theoretical part, which, however, is essential for training in the practical area.

The next part, which is connected with physical principles and construction of sensors, is the ways of their utilization. The combination of these two areas of education will secure the selection of the suitable sensor for the given activity. Education in this sphere already pre-supposes thorough familiarization with concrete types of sensors being used in the given armies. Education also includes practical work with sensors, instruments and installations, which are assigned the task of evaluating information from the area of interest.

The field of utilization of sensors and their suitable selection is a very complex part of education of both the individuals and units. A variety of factors, which it is necessary to take into account during the decision-making and setting the parameters of the selected sensor (for example temperature, weather conditions etc.), play their role here.

A very important role is played by optimal distribution of sensors. The requirement is an effective collection from the sphere of interest. Incorrect distribution of sensors means a loss of information, which is, in the IW, the main weapon. In the past, distribution of sensors used to be the matter of intuition of the commander. Nowadays, however, effective algorithms and methods, which

ensure optimal distribution of sensors, are appearing. The use of these algorithms, however, is conditioned on the knowledge of them. For that reason, this form of education must also be included in training of military personnel. Only then will the optimal distribution of sensors in the area of interest be guaranteed.

Another field of education, which also is closely tied with education in the field of sensors, is understanding the principles of activity of sensor-interconnected installations and networks, including the way of transmission of a digital signal and its coding.

In the past, information used to be obtained through the activity of agents and spies (that is, the people who act directly in the environment of the enemy); today the main effort is concentrated on electronic means, emitting secret data into open space, penetrating secret information systems and operating in them remotely, for one's own benefit.

Obtaining information transmitted by the enemy is the main weapon of the IW. This is what each of the adversarial sides is attempting to achieve. Being able to listen to important information of the enemy means a great success. Therefore, much time is allocated to the transmission of such information.

The resistance of electronic devices and networks against monitoring (that is, unauthorized utilization of foreign data) is becoming one of the primary requirements of all modern armies. It is, therefore, necessary to suit the form of education of military personnel to this trend.

Education must focus on understanding the principles of communication devices, and transmission of data between them. The emphasis will be put on securing one's own data and monitoring the data of the enemy. With this is, to a significant degree, connected transmission of a digital signal and its coding (possibilities, means, principles, forms). Selected fields of electronics, electricity, computer networks and cryptography must, therefore, be a part of education.

The IW also concerns computer networks and tapping into information systems of the enemy. Education, therefore, must also address this area. The desirable effect, to which the quality education will particularly contribute, is the defence of one's own systems and penetrating the systems of the enemy.

In the IW, similar to the rest of the forms of war, at least two enemy countries are facing each other. Each country must take into account that the enemy has similar knowledge and sequence of activities. For that reason in particular, quality education and training are very important for the successful conclusion of the war. Only professionally trained personnel are the guarantee of quality conduct of the fight, with minimal danger of errors. Tied in with this subject is also the question of disinformation. This mode of fight may be very successful and, therefore, it is suitable to allocate much space to it in the field of education and preparation for it.

The condition for conduct of the IW is availability of peak technologies in the field of electronics, experienced and thoroughly prepared human potential, and thorough knowledge of the enemy and his possibilities in the field of the IW. Therefore, the indispensable part of education must be the subject of technical means of the enemy, mentality of the members of his armed forces, customs and ways of utilization of information in peace and during the fight.

All the above-described factors are indispensable for education of both operators and soldiers, who are participating in the IW. It is important to not underestimate any sphere of this education. Professional education and training form the basic element of success in the IW.

2.2 Training

Training is complementing education, in particular in the practical aspect. The figure 3 depicts some basic elements that are indispensable in the field of training. The emphasis is, in particular, on installation of sensors and communications means and their diagnostics.
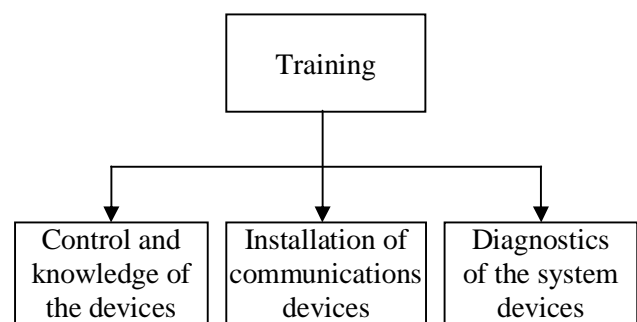

Fig.3 Training areas for the Information War

Achieving control over, and thorough familiarity with, all the devices and equipment, and their correct use, is the basic phase of the training. Complicated construction and the way of using the instruments and installations demand wide-spectrum education and training. The important thing is to concentrate on all the basic and unpredictable situations, which can occur in the real fight. Due to the action of the enemy, the equipment may, for example, be

damaged and it may function improperly. Training of the operator must focus on solving similar situations.

The next point of training is mastering the installation and camouflaging the sensory and communications means in various types of the area of interest. In particular, it is important to focus on the optimal distribution of sensors. Sensors are the main sources of information; their correct functioning is, in the IW, fully indispensable.

Installation also concerns the means of communication. The area of transmission of the digital signal and its coding have been mentioned in the chapter about the individual forms of education. Required is the fast establishment of the connection between the sensors and communications means, with no tapping in by the enemy. An inseparable part of the installation of the sensor and communications means is their camouflage. It is fully mandatory that these devices are not discovered by the enemy. Their discovery by the enemy may have catastrophic consequences. By their destruction, indispensable sources of information are lost.

In the next part of training, the subject will be the ability to use the built-in diagnostics means of the systems. The current sensors, instruments and complex weapon systems are literally overflowing with electronic elements and microprocessors, which may be damaged or altogether destroyed by the influence of strong electromagnetic pulses or chemical agents. The instruments are usually composed of built-in modules, which it is possible to replace in the case of malfunction. The diagnostics of the instruments will make it possible to determine the damaged modules, which must be repaired or exchanged. The operators must perform the diagnostics of all system means before their installation, but even in the time of their use. This is why this area of training is very important; operators of instruments and installations must be able to utilize the available diagnostics means and solve unpredictable situations, which may occur through the action of the enemy.

3 Conclusion

The 21st Century is being connected with a mighty onset of new forms of fighting, which we summarize under the term of the Information War. The result of this "humanitarian" war is not the loss of human lives, but only the loss of the capability to carry on any fighting activity.

Lagging behind in the area of development of information technologies and underestimating this form of fighting may prove, in the future,

detrimental. The foremost experts, it turns out, liken the effectiveness of the IW to effectiveness of the weapons of mass destruction. The IW may have various forms - from inconspicuous, hidden manipulations of data, all the way to a total failure of automated information system and loss of fight-worthiness of armies.

The IW must view education and training of military professionals in a wholly new way. Considering the complexity of construction and the ways of utilization of the monitoring devices, it is mandatory to be interested in, and look for, the best possibilities and forms of education and training. The present contribution is attempting, in at least general terms, to suggest the individual directions, in which both education and training must travel.

Education of similar character has not been, so far, common in armies, but the present development of digital technologies will certainly demand it. Every modern army, which does not intend to underestimate this new form of fighting, that is, the IW, must create for itself a quality system of education and training, both of military and civilian personnel.

References:

[1] Hluboček, *Modern Information War in the Digitized Battlefield* (n*ovodobá informační válka na digitálním bojišti)*, Computerworld, No.11, 2000, pp. 20-22.

[2] Kaucký, *The Information War at the dawn of the 21st Century* (i*nformační válka na počátku 21. století*) [online].
URL: <http://www.atmonline.cz/>.

[3] *Networked Enabled Capability* [online], Version 1, 2004. URL: <http://www.mod.uk/>.

[4] Alberts, Garstka, Stein, *Network Centric Warfare* [online], CCRP, 1999.
URL: <http://www.dodccrp.org>.