Military Education and Training for Information Warfare

Miroslav Hopjan

Petr Stodola
University of Defence, K-269
Kounicova 65
61200 Brno
Czech Republic

miroslav.hopjan@unob.cz / petr.stodola@unob.cz

ABSTRACT

The paper deals with the Information Warfare issues from educational prospective, what should be done to use, develop and employ the M&S.

Our current understanding of possible impact of technology development to warfare, particularly to command and control infrastructure in Information Warfare is presented. This has been topical problem for some years, especially when modern technology can become in terrorists hands effective weapon directed not only against protected military systems, but also against vital civilian systems that can endanger many people when not working properly or when misused.

The main part describes different forms of information warfare, attacks and appropriate countermeasures. This places certain requirements to training and education facilities including modelling and simulation infrastructure. Different access is necessary during basic officer training, college study, and staff training phase. Command and Control Information Systems (CCIS) are currently in introduction phase within the Czech Army. Even if CCIS will be fully exploited during CAXes we still will be missing sound base, both in model and scenario areas to prepare commanders properly for future challenges.

Another focus is aimed to sensor area, in terms of delivering necessary background in physical principles, wide spectrum surveillance, signal coding and transmission, sensor networking, unaffected failures, jamming and tampering.

1. INFORMATION WARFARE / NETWORK CENTRIC WARFARE / NETWORK ENABLED CAPABILITY

The headline brings up three different terms. Despite the Information Warfare was chosen as the representative for the rest of this paper all three are closely interconnected, all of them are important for future force structure, the way we are going to fight in future, as well as for the way we need to train military personnel to be prepared for future NATO missions. In fact, we are going to find better ways to educate and train staff that will assist our military in Network Centric Warfare implementation phase. This means quite small steps towards fully networked and NATO interoperable military, especially when leading NATO countries introduce new findings in military at faster pace. We do not want to leave the ground and concentrate on possible cyber wars in future, we want to adapt the way how commanders and technical staff are being trained and educated to near future needs, taking into account also mid- and long-term trends and emerging technologies.

Paper presented at the RTO NMSG Symposium on "Modelling and Simulation to Address NATO's New and Existing Military Requirements", held in Koblenz, Germany, 7-8 October 2004, and published in RTO-MP-MSG-028.

Network Centric Warfare (NCW) represents a powerful set of war fighting concepts and associated military capabilities that allow warfighters to take full advantage of all available information and bring all available assets to bear in a rapid and flexible manner.

The tenets of NCW are:

- A robustly networked force improves information sharing
- Information sharing enhances the quality of information and shared situational awareness
- Shared situational awareness enables collaboration and self-synchronization,and
- enhances sustainability and speed of command. These, in turn, dramatically increase mission effectiveness.

NCW concept (see Figure 1) emphasizes real-time links allowing distribution of sensor data to executive bodies, to combatants and weapon systems.

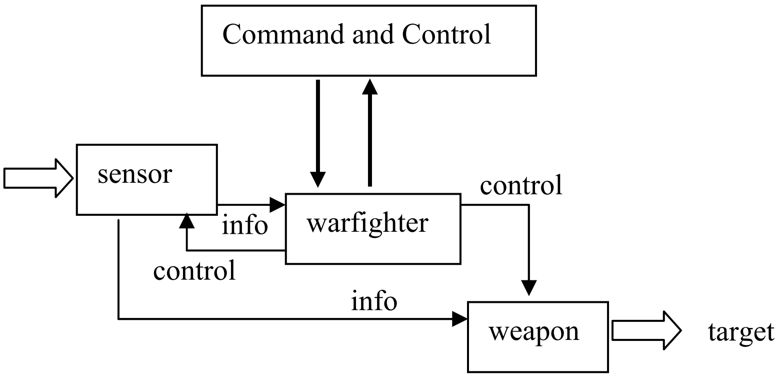

Figure 1: Network centric concept

The term **Network Enabled Capability (NEC)** announces British initiative following the same goals like Network Centric Warfare. The initiative further develops NCW with focus on development of

- **Structures and Process**

Flexible force structures to support smaller, task-based teams
New roles are needed to support the use of information
Increased use of Reachback to reduce in theatre footprint

- **Concepts and Doctrine**

New doctrine to support real-time, collaborative internetworking and Effects Based Operations.
New doctrine to support smaller, task-based teams
Doctrine to include new styles and ways of command

- **Training**

New ways of team building for ad hoc task-based groups (to build trust rapidly)
Training to participate in ad hoc task-based groups.
New skill sets for personnel within ad hoc task-based groups.

- **Equipment Capability**

An agile strategy for delivering and maintaining NEC
Applications to make best use of information
Treating the infrastructure as a single concept.

- **Sustainment**

An appropriate equipment support and supply regime for the infrastructure as a whole.
Agile logistics to support ad hoc task-based groups

- **Personnel**

New roles to support greater availability of information
Making greater use of commercial expertise.

Information Warfare (IW) is new form of battle in turn of millennium. Information comes to be the most powerful modern weapon. Efficiency of using weapons systems is dependent on quality, credibility and seasonableness of information about enemy.

IW is waged in the information domain. If it is unleashed in full strength its sequences can be really fabulous. It has effect on decrease soldiers' morale and battle cogitation, and in this regard it has direct effect on combat efficiency all army. Notable experts in this area look for more efficient and effective way of this form of war.

From experience of armed conflict in which elements of IW were used experts suggest if IW will be correctly and skilfully waged decisive success can be reached without using of classical weapons, even without human lives losses.

The term IW is largish. It includes activities in communication area, encroachment on computer networks of information systems, access and invasion of data network, interference with reconnaissance systems and devices communication, and interference with military command and control systems.

Besides that, all public media (TV, newspapers, radio) can be used (and abused) to gain public support for military action, to affect the morale of combating forces, civilian people in countries involved or in theatre, etc. In following text, we stay limited mainly by technical experts responsible for CCIS or sensor network.

All possible forms of the IW are not exactly known yet. Unlike other known forms of war it is hard to identify the activities beginning, to determine accurately their range, and to recognize which elements of information systems were attacked and form of this attack, to assess the damage, etc. At first sight attack of no significance to certain part of large information system can cause "chain reaction" effect of which can be catastrophic.

1.1 Use of modern resources

The way of army command is changing very quickly. Contemporary battlefield is congested with electronics and the frequency spectrum is charged with all kinds of signals. Electronic devices help commanders in the decision making process, and increase the effectiveness of using weapons. Commander get accustomed in the digitised battlefield quickly because in practice they ascertain how accomplished the situation awareness is, also from distant interest area.

Therefore the situation happens to be critical when commanders forfeit the remote command ability, as they have to take an emergency action and start to use the old way of conducting reconnaissance and command. Likewise the modern weapons are dependent on electronics and cannot work in old mode.

General truth is that the key factor for modern way of combat action consists in capability, collection, processing, propagation and usage of information on enemy armed forces in conjunction with restraint of enemy's information collection on friendly forces and action against them.

Fundamental prerequisite for victory in the IW is arming of units by commensurate resources allowing a transmission, receiving and display of digital information. Data networks that are built up in all modern armies, allow very quick collection, sorting, and distribution of battle information. Systems and resources perfection allow automating many routine operations.

However perfection usually entails complexity. And more complex technical equipment means less human ability to check devices functionality. Embedded diagnostic circuits common in all new electronic devices should be able to detect failures and standard value variance. But these diagnostic circuits cannot cope with skilful data manipulation on input or output.

1.2 Information Warfare Weapons

Main weapons in the IW are information resources and technologies used to fast and concealed activity to enemy military and civil information systems aimed to disturb or preclude his activities and carry out the contents and form manipulation of carried information.

The IW can be carried out in a stand-alone way that means without using common weapons of war, resources and way of armed battle, but also in accordance with traditional combat action.

The IW is not necessarily oriented to material targets, but to information and data objects (that means to all structural elements of information networks, resources for data transmission, computers including all kind of data medium). The activity does not always end up by direct physical destruction of the material base, live forces and weapons of war.

Facilities and effectiveness of the IW still increase according to grow of complexity, operational facilities and microprocessor propagation in complex weapon systems and sensors. These facilities in the hands of experts can contribute to increased performance of weapons.

1.3 Information Warfare Faces

In the IW various means are used, particularly sophisticated tool can be computer software. It is accomplished by setting special virus or Trojan code to various computers, their activation can be remotely controlled.

Experts develop special resources that can create intensive electromagnetic impulses destructing basic semiconductor structure (microprocessors, integrated circuit, computing memory, etc.), all electronic circuits but also various insulating materials using in computers, computer networks and its accessories. Especially sensors are very vulnerable to such weapons; their better resistance is always trade-off with desired high sensitivity.

Experts also develop various matters inductive creation different chemical and biological reaction with harmful effect on fractional structural element. There resources can cause much faster ageing of devices, corroding process or decrease of quality, durability and consistence of various materials.

The IW action can start before the combat action or it can make compensation for it (on condition that the IW will be effectively controlled).

We do not know whether TV news or newspapers articles coming every day are mere information without any other intensions, or whether the facts were falsified, the topic was chosen, or the wording should bias the meaning with very specific goal by IW experts. In fact, we might be under IW attack every day.

2. EDUCATION AND TRAINING

Only extensive experience personnel and operators assure effective wage of battle. This paper is limited in scope to technical part of the topic, we try to draw a broad idea how to prepare technical experts for IW operations.

Aforesaid facts and properties of the IW have to be mirrored in military education and training personnel. Because more and more percentage of military (in fact, civilian contractors are increasingly involved, too) are becoming users of communication, information, reconnaissance, and surveillance systems their education and training is an important issue at all military hierarchy levels.

Considering of extensive technical development it is obvious that education and training is necessary to be continuous process. Though there were several armed conflicts with elements of the IW this form of combat is still at the beginning. New and improved facilities, principles and technologies are emerging, new techniques and doctrine of their use are being developed, and it is important to acquaint military and civilian personnel with them.

Increasing capabilities and proliferation of the Information War facilities also put higher demand on developing and implementation of countermeasures, increased robustness of systems and networks. It is necessary that everyone who participates in war can employ an adequate, rapid and mistake-free response to possible enemy actions. Component part of individual and collective training should be not only correct knowledge how to operate a device and equipment but also flexible and imperturbable reaction to both its own errors and malfunction, also to those caused by enemy's activity.

Time interval between individual course and form of education depend on many factors.

Position and task performed are important when building the appropriate education or training course. Because there are many forms of the IW it is not simple task to create and design ways and forms of training. Following text will try to pursue basic areas of education and training focused to IW operations.

2.1 Education

Figure 2 shows several basic areas of education that all signal corps officers should go through. Emphasis is put on comprehension of physical principles and working principles of sensors and communication resources.

Role of sensors in NCW conditions becomes more distinct as they are supposed to release their tight links to weapon systems. Independent sensor network does not, of course, mean totally separated sets, or general, WAN-like network. Figure 2 outlines the most important issues in area of sensors education:

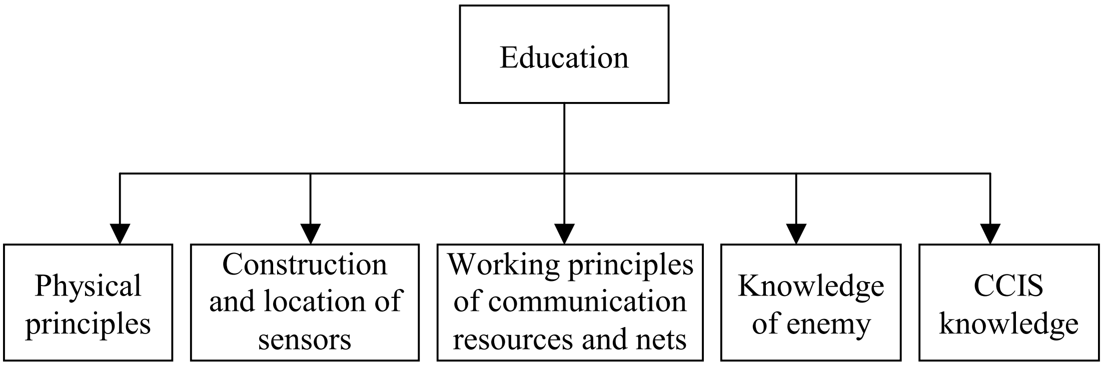
Education
Physical principles
Construction and location of sensors
Working principles of communication resources and nets
Knowledge of enemy
CCIS knowledge

Figure 2: IW specific areas of education

- Comprehension of basic physical principles concerning emitting, scanning and evaluation various kinds of energy in broad spectrum.
- Knowledge of military systems used as IW tools is directly necessary for effective equipment and devices operating in the battlefield.
- Scanning procedures and following results evaluation. Individuals must know the equipment and devices for scanning energy and signals well. Further more important is to be able to use mathematical methods for processing of scanned signals.
- Construction, usage and location of suitable sensors. Because they are the main information source, and within networked battlespace, they should become independent on weapon platforms to allow building of large-scale flexible and inexpensive intelligence networks. Following questions are of particular importance:
    - Choice of suitable sensors, their performance, their sensitivity/sustainability, endurance under conditions of enemy's IW attack, weather and climate insusceptibility,
    - Location of sensors, ability to deliver them to the area of interest, the network topology, desired orientation, possibility to control their activity,
    - Data transmition rate, compression, encoding and decoding, sensor data fusion capabilities.

Another important IW related block includes computer networks and CCIS security:

- Physical implementation, topology, robustness, protocols, network management,
- Data security (both technical and administrative arrangements) and security management, data backup, operating system management and recovery,
- Malicious software detection and system protection, sniffing, traffic monitoring, cryptography, interception detection, infiltration into enemy's systems, disinformation, network attacks.

These topics are already today receiving fairly good amount of attention, however security of networks and information systems is difficult to achieve, these problems continue to set limits for networked military systems. Current study programmes reflect to certain extent technical issues of NCW and IW, but are still missing concentrated effort to adopt our education to future needs.

2.2 Training

The decomposed training and education have limited use in growing complexity of information network on the battlefield. Theoretical part of study is not always ballanced well with practical training ("train as we fight", "train as we work"). Our current simulation tool (OTBSAF) used for Bn/Bde staff CAXes is to be supplemented with CCIS network during next year. This is a challenge for developers to implement for training purposes modules allowing simulation of IW conditions. Another important enhancement should be device simulating real communication network properties.

The flexibility we need to attain cannot be built without sound theoretic base and experience from exercising using the systems. This shows that our current education system using traditional scheme need to be changed in favour of more frequent distance learning based pattern.

As an example of training for NCW/IW here is an outline of concrete proposed course (Figure 3). Its topic is installation sensorial and communication resources and their diagnostics, the system mentioned here provides ground surveillance.

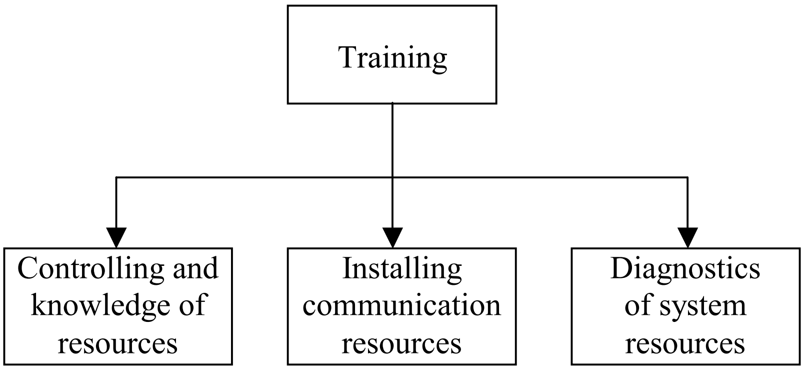
Training
Controlling and knowledge of resources
Installing communication resources
Diagnostics of system resources

Figure 3: Sensor training outline

Operating and complete knowledge of all resources and devices and its correct usage is basic phase of training. Complex construction and way of equipment and devices usage requires wide-spectrum education and training. It is important focus in all basic and unforeseen situations that can happen in real battle. Activity of enemy can be cause of damaged equipment or its malfunction. Operator training must be concentrated on solving similar situations. Effective training would be possible only when employing complete system, in real terrain, which is costly solution. We need to model this activity to allow complex staff training, also to give a feedback concerning the sensor placing.

Next point of training is installing and masking of the sensorial and communication resources in various types of interest area. Stress should be put on optimal sensor location. Sensors are main source of information and their correct working is vital for successful military activity.

Installing relates to communication resources, too. Digital signal transmission and encoding was mentioned in previous chapter as one of theoretic topics. Fast connection establishment between sensors and communication infrastructure is required.

Integral part of installing sensorial and communication resources is their masking. It is necessary that enemy will not discover these devices. The discovery may result in loss of important information input, or, worse, possibility for enemy to insert into our network confusing information.

Here is another point to involve M&S to credibly simulate harsh combat environment, also to keep users of the system alert, teach them to verify their information.

Important capability of modern sensors usage is embedded diagnostic of system resources. Overloading such systems with microprocessors and other electronic circuits makes their use as simple as possible.

This, in turn, can lead to be damage or complete destruction by strong electromagnetic impulses or chemical agents. Diagnostics of the equipment enables to identify faulty modules necessary to replace. Operators must execute diagnostic of all system resources before its installation but also in real working. Diagnostics of sensor network placed in real terrain area of training can discover some of possible problems but will hardly yield sufficient information like the sensor network under IW attack.

This example shows what simulation and stimulation tools will be necessary for effective training. Despite we have no such systems in routine use today it is high time to plan our tomorrow's training today.

3. CONCLUSION

The Information Warfare is something that can bring glorious success as well as heavy losses. The result of losing ability to control any combat action is devastating despite saving human lives. Equal risk we face from terrorists with explosives can happen any time at any place without any tangible evidence. Backwardness in information technology development and deprecation of this form of battle can be beyond in future. Experts compare effectiveness of the IW to effectiveness of mass destruction weapons. The IW has a lot of representations – from discrete hidden data manipulation to total breakdown of automated information systems and loss of fighting capacity.

The IW must convert education and training of military professionals into new process. In consideration of complexity of construction and ways of usage monitoring resources it is necessary to employ the best facilities and forms of education and training. This paper tries to show some preliminary steps in that area.

The problem is not merely new technology understanding and using, a lot more has to be changed in doctrines, procedures, and in people's mind. To help in this process, there is blooming modelling and simulation industry to learn consequences of intended changes, and to allow training in situations that are difficult to invoke in real.

We are trying to match increased demand for knowledge and skills appropriate to IW operations to economy reality that pushes to downsizing and effectiveness. The process of development and fielding of modern weapon systems, as well as new C4ISR systems, is a long-track-run. This paper tackles small part of task that the University of Defence will have to solve in close future. Having to shorten contiguous education periods we must prepare more tailored courses employing simulation technology, eLearning, and distance learning.

The more we rely on technology the more capabilities we gain, though, at the same time we open bigger part of our vital infrastructure to possible IW attack. This risk is impossible to exclude, because emerging technologies are likely to be exploited by our adversary anyway. Nowadays, when the gravity centre of war against terrorism is in combating fairly low-tech enemies, there is still threat from highly educated freely financed groups of exploitation any vulnerable point of our technical infrastructure, civil or military.

REFERENCES

[1] HLUBOČEK, Vladimír. *Novodobá informační válka na digitálním bojišti*. Computerworld, May 2000, no. 11, s. 20-22.

[2] BASTL, Martin. *Co je informační válka?*
URL: <http://www.sever.cz/text.asp?clanek=1315>.

[3] *Informační válka na počátku 21. století* [online].
URL: <http://www.atmonline.cz/news/2004/unor/240204b.htm

[4] Networked Enabled Capability, Version 1, 2004, http://www.mod.uk/linked_files/issues/nec/NEC%20Pamphlet.pdf

[5] Alberts, Garstka, Stein: Network Centric Warfare, CCRP, 1999, www.dodccrp.org