Wireless Military Communications - NNEC Enabler

Miroslav Hopjan, Zuzana Vranova
University of Defence, Department of Communication and Information Systems,
Kounicova 65, 60200 Brno, Czech Republic
Miroslav.Hopjan@unob.cz, Zuzana.Vranova@unob.cz

Abstract. The paper discusses the NATO Network Enabled Capability concept, mainly from the communication point of view. The changes involve complete new requirements on the role of command and control to increase flexibility and effectiveness. Integration of Modeling and Simulation with Command, Control, and Information Systems increases the number of risks but it promises to leverage the projected capability and interoperability.

Keywords: NNEC, simulation, tactical communication, CCIS.

1 Introduction

This paper does not introduce new technological solution in wireless communications, the point of view is closer to the customer side of the house – how to use the emerging communication technologies in an optimal way supporting the concept of NATO Network Enabled Capability (NNEC) which emphasizes the role of information superiority in modern warfare. The aim is to evaluate number of aspects when implementing this technology in the Czech Army. What role is adequate for contemporary microwave devices, why the implementation is delayed, what risks must be outweighed by benefits of these solutions. Communications networking is the clearly visible part of the solution, and suitability of selected, mostly wireless communication approach, is discussed.

Although it is not the core functionality for Command and Control Information Systems (CCIS) it is apparent that NNEC encompasses also Modeling and Simulation (M&S) capability. These two domains have developed different architectures, standards but further progress of one system is related to the other. Modern wireless communication means promise to fill one gap between these two worlds.

This article tackles two oncoming trends:

- raising demand of (wireless) communication means to individual combatants to share the knowledge (operational picture)
- integration of M&S capability into CCIS

2 The Need of Flexibility and Agility

The processes of changing doctrine, force structure, inevitably accompanied by change in procedures and equipment, called “transformation” is symptomatic for all

armies recently balancing the East-West military powers trained and prepared for another World War. While not completely abandoning the imperative that armed forces of particular country must be prepared to defend the state territory from massive attack it became clear that building and maintenance of military forces according to Cold War era would be prohibitive simply for economic reasons.

So, instead of traditional, fixed unit organization that is both costly to move, accommodate, supply, protect, and slow to maneuver we are trying to enable any possible task force, autarchic enough for months-long deployment, and tuned for so called Effect Based Operations according to current task, adversary, and conditions (Mission-Enemy-Task-Time-Civilians). It is apparent that in case of technological superiority the enemy will use more concealed, guerrilla-like ways of combat. This does not exclude using the same contemporary technology by the enemy whenever it is effective. Building such modular, well trained forces, capable of deployment anywhere in the world as well as acting as an element of territory rescue system, or doing police job in unstable regions, is difficult from a number of points of view. At the same time, implementation of NNEC principles enables getting over limits flowing from traditionally strict military organization; improved access to information both concentrated in databases and gathered by front-line sensors and units together with increased decision autonomy (Loosely Coupled Management Process [2]) enables creation of informal networks. Using Complexity Theory [1] information entropy of such system is lower, system with non-centralized decision making and information sharing allows all parts to learn and adapt, see Fig. 1.

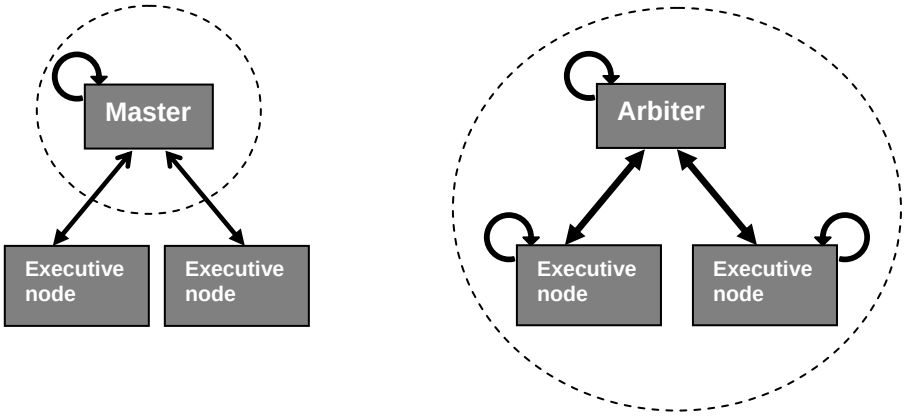

Fig. 1. Loosely Coupled Management Process
The left hand side depicts the traditional organization where subordinate units (generally executive nodes) perform tasks, higher commander (master) is the only learning and adapting one (dashed circle). Sharing the information and decision power is illustrated on the right side.

Obviously, the world is not only black and white; the level of autonomy varies depending on current situation. The technology level that enables extensive information sharing makes not only the decision making process at lower level more effective and optimal, it enables the transfer of information in opposite direction, too.

The feasibility of getting detailed and timely information from front-end units may be tempting for high-level commanders to skip the chain of command and apply direct control.

2. 1 The NEC Concept

The simplified view how the network concept can contribute to enhanced operational capabilities is depicted in Fig. 2. New capability in such complex environment cannot ensue only from extended technology level as this creates new challenges in related domains. For example, extended range and higher precision of weapon system is undoubtedly operational advantage. But if any delay occurs in communication, the IFF (Identification Friend or Foe) systems are not fully interoperable, or different procedures of decision making process do not support the timely mission plans alignment we have a problem with euphemistic name "friendly fire". If components in all layers are not in accord then an individual improvement can be disturbing, even risk increasing factor.

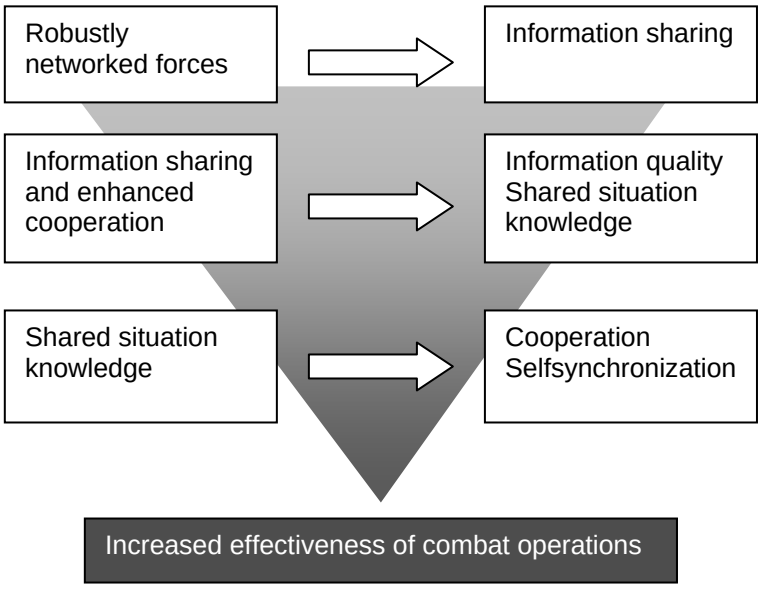

Fig. 2. The NEC concept

The NEC does not mean simple network layer extension vertically and horizontally (vertical connection of Ground Forces and Air Force communication and information systems, horizontally - extending connectivity to smallest units); according to [3] there is an impact on all domains:

- Physical (tactical) – sensors, surveillance systems, data acquisition
- Information (operational) – information analysis, tools and models supporting decision making
- Cognition (military strategic) – deep understanding, highest decision level

- Social (affecting all individuals)

The changes will affect not only technical infrastructure but also the organization structure, decision making and planning procedures as well as the education and training.

2.2 Bringing Modeling and Simulation closer

Both CCS and military M&S systems have their own long history. Information technology serving in commander decision process must not increase notably the weight, complexity, power consumption, and maintenance staff as it might easily become ballast increasing vulnerability, requiring special treatment and long time to process raw data. This was absolutely true for high-resolution virtual simulators as well as for computation intensive staff simulators requiring special hardware, months or weeks to create terrain database and exercise scenario, and experienced personnel to run the simulation. When low-cost PCs connected in a network became appropriate the hardware limits could be overcome.

There are many problem areas where we still have not reached final solution; standards should be developed to allow seamless integration of M&S systems within overarching NNEC environment.

The ACR technology lag is quite apparent in the communications domain. Well, it is difficult to get any satellite communication except the contracted one but the NNEC concept was implemented in information systems and communication domain rather with respect to legacy systems than with broader, future vision.

Such a goal has not been pronounced by the ACR representatives yet but thee future development should continue in diminishing the difference between the combat and training by embedding the M&S into equipment. Despite this raises many new questions how to eliminate related problems it is clear that modern wireless communication systems will be the key enabler of new capabilities.

3 Aspects to Consider

Let us make closer look at problems accompanying the NNEC concept realization in the Czech Army. Based on experience from previous projects we should identify risks, they are mutually related:

- Political risks – despite there is limited chance to avoid wrong political decisions their impact on technology can be eminent (further development costs, interoperability, strong bond to certain supplier, etc.),
- Economical risks – life cycle cost of a system is extremely difficult to plan, also poor user specification and changing requirements often produce collateral damage when resource shortage stops or puts behind linked projects; this comes to unsatisfactory functionality, creating new demands on manpower or growing system obsolete
- Technical risks – when implementing new technology it must be thoroughly analyzed whether this technology is mature enough to avoid

life cycle shortening due to reaching its technical limits; is it likely that this technology will be standardized?

3.1 Bandwidth

Building the communication infrastructure using traditional SW tactical radios may become fatal barrier when involving sensor grid such as UAVs or integrating simulation assets. There is backbone network using modern commercial technology capable of transferring satellite imagery and databases in no time. How can we deliver and process data from numerous ground sensors? ZigBee rather than WiFi could be the right solution, although there is not capacity reserved in today's communication infrastructure. The ACR wireless tactical intranet is capable of sharing situation reports, short messages, and orders, nothing else.

3.2 Interoperability

Before any new technology is considered for military implementation an analysis of its impact on acknowledged standards or possible need to create new one must be carried out. The standardization processes are NATO is somewhat cumbersome in areas where vital functionality is not affected. Whenever possible, international commercial standards are adopted. Communication parameters belong to critical areas with little freedom to use different coding, data model and formats, frequency bands, modulation, etc.

On the other hand, the M&S area was for many years “rear-echelon” activity. High intensity warfare was not favorable environment for building deployable training facilities, and technology limits did not allow truly portable systems. Then, ground and air systems were isolated; the same was true for combat and logistics. Tactical and operational simulators were useful for early training phases, rather than for mission planning or mission rehearsal, which becomes an important feature today.

When networked simulations started to play important role in NATO activities standards emerged to allow even global and secure multinational exercising.

Strong effort is being spent now to find an appropriate architecture, data models, and other aspects that would enable seamless CCIS and SIM integration.

3.3 Robustness

The first most important requirement on the military communication channels is high probability of successful message delivery. In terms of the network topology and management there must be redundant or backup infrastructure, and network condition monitoring to keep the reliability high. Depending on classification level and unlikely in the public Internet, mostly dedicated, and therefore expensive, channels e.g. satellite or radio-relay links are necessary.

3.4 Security

Information security should minimize access to knowledge to unauthorized system user while not affecting the overall capability (Need to Know versus Need to Share). Today's closed, individual service owned CIS do not support multi-layered information security concept, and there are mutually incompatible cryptographic products in use. Secure Communications Interoperability Protocol (SCIP) will be necessary to interconnect system elements. Wireless data network solutions such as WiFi, WIMAX, or ZigBee are becoming respected players after proving their suitability for classified networks.

Security is a big issue; when connecting voice and data networks together plus linking intelligence databases further increases the security urgency. Attacks against military networks are still mostly proof-of-concept but this does not mean that such a weakness will not be exploited in critical situation when the advantage can be maximized.

We pay considerable attention to data channel encryption, still, the security is not just about unbreakable cipher – it is alarming that stolen computer discs from military installations, sometimes with data extremely useful for the adversary, can be bought on markets in Afghanistan.

3.5 EW Insusceptibility

Electronic warfare has changed the view of military operations due to its potential to gain a superiority using smart, high-tech means. Sometimes the cutting edge technology is of little help against enemy that uses low-tech means or an effective and inexpensive countermeasure appears soon after spending fortune on technologically advanced system. Defence research and development projects have been drivers for commercially successful products, the opposite direction of valuable solutions propagation is analyzed eagerly too. Though, the cost concerns cannot be overlooked.

The intense wireless computer network expansion left the military decision makers untouched till the security concerns prevailed. Still, military implementation must look farther to balance the good and bad. Overcoming the security issues of wireless communication there is still problem of traceability of the transmitter; accuracy of which increases in higher frequency bands. Another example is the painful Improvised Explosive Devices (IED) problem. To disable remote control of IEDs powerful broadband jamming must be used.

Satellite communication becomes inevitable when forces are deployed abroad, not only as a home country link but also in the theatre. Today's doctrine did not count on vast distances covered by small, tactical units; their radio reach is insufficient, especially when operating in mountainous terrain. But, what risk we take if contracted SAT connection can be tracked by an enemy connected to the Internet?

3.6 Small Footprint

The measure of effectiveness of any military campaign compares the effect of armed units with total costs. While lack of important material can slow down or even

disrupt operation plans, and therefore certain surplus is preferred, opposite case increases the need of transport capacity, affects the mobility, requires more people and time to move, maintain, and protect the logistics tail. Supporting units are more vulnerable in low intensity conflicts when fewer personnel are operating in large territory. Generally, the relationship between new technology and its footprint is nonlinear, depending on the technology maturity; users often perceive in the beginning that new functionality is well balanced by the additional weight, shorter battery life, and high complexity affecting reliability and reparability in harsh environment, ease of use when under stress. The increasing networking and computer control trend is faster than progress in lightweight, high-capacity accumulator or fuel cell technologies. Data communication is taking over the traditional voice communication channels with the aim of unified, simple, and new possibilities offering infrastructure.

4 Conclusion

The Army of the Czech Republic is facing new challenges related to doctrine change, coalition bonds, global security risks, and latest technology achievements. The traditional territory defence has evolved into highly mobile expeditional units. The NNEC concept striving for information superiority allowing higher combat effectiveness places new requirements on communication infrastructure (not only that, the impact will be much more complex) in terms of connectivity, capacity, and security. The short term goal is seamless connection of link and wireless encrypted communication channels. The system is scheduled for security certification but we cannot include multiple security levels as requested. Current solution of wireless "tactical intranet" would not handle the sensor grid data volume. Integration of M&S and CCIS increases the demand on the network bandwidth while enabling training and mission rehearsal in combat zone, even different options evaluation during the decision making process will be possible.

References

1. Moffat, J.: Complexity Theory and Network Centric Warfare. Washington DC, USA: CCRP Publication Series, 2003.
2. Atkinson, S.R., Moffat, J.: The Agile Organization. Washington DC, USA: CCRP Publication Series, 2006.
3. Smith, E.A.: Complexity, Networking, & Effect-Based Approaches to Operations Theory and Network Centric Warfare. Washington DC, USA: CCRP Publication Series, 2006.