MODEL OF A TACTICAL COMMUNICATIONS SYSTEM IN THE AGE OF CYBERTERRORISM

Ernest Lichocki

Abstract:
On the modern battlefield, a tactical communications system constitutes a complex and very complicated set of possibilities. Modern network-centric warfare is extensively dependent on tactical communication – radio transceivers connect soldiers, units, staffs, weapons systems, ships, helicopters, unmanned aerial vehicles, and combat aircraft..

DOI: 10.19197/tbr.v17i4.344

In Lieu Of Introduction

A communications system is defined as "an organisational and technical set of forces and means of communications and information technology, answering to the demands of command and control over the means of destruction, to the nature of conducted operations, and to the tasks performed by the troops". At the same time, it should be emphasised that the term "communications system" is broader than "communications network[1]", although the two are commonly treated as interchangeable.

On the modern battlefield, a tactical communications system constitutes a complex and very complicated set of possibilities. Modern network-centric warfare is extensively dependent on tactical communication – radio transceivers connect soldiers, units, staffs, weapons systems, ships, helicopters, unmanned aerial vehicles, and combat aircraft.

Why National Cryptography

[1] Communications network – "sets of closely related forces and means of communication developed (deployed and operating) according to a uniform plan in a specific area in order to ensure the exchange of information within the system of command and control over the means of combat" (J. Mazurkiewicz, Leksykon łączności wojskowej, AON, Warszawa 1996, p. 176).

The Armed Forces of the Republic of Poland conduct international military operations together with a dozen or so countries, encountering problems related to the interoperability of communications systems. It is almost as if each country had its own radio transceiver with its own capabilities and crypto chip. The United States, the largest user of tactical communications systems, promotes Harris radios as the de facto standard, and many potential users believe that by purchasing these radios they will solve their interoperability problems on the battlefield. Communication with all countries except the United States remains a problem, as the US only shares cryptographic doctrines or details under very special circumstances (e.g., when its particular interest is at stake)[2]. It is not possible to obtain or purchase class A tactical systems and radios reserved for the US Army, only lower class B.

In the 21st century, cyber-attacks are becoming bolder, more cunning, elaborate and dangerous, exposing the need for very strong cryptographic protection. It is preferred to put full control over these matters in the hands of the state in order to ensure the elimination of "backdoors" and cryptographic traps. If the tactical communications system does not offer strong protection against cyber-attacks and deliberate disruptions, it fails to meet the requirements of the modern network-centric battlefield[3].

The state security services or national security agencies of some countries go very far to ensure the protection of their countries' information, and it seems that they have access to other countries, even those that are members of NATO. In The Economist, published on 14 September 2013, a number of articles explain how the National Security Agency works to ensure it has access to as much information as possible. These efforts include ratifying standards that are weaker than one would normally expect (e.g., random generators that are not so random), and collaboration with US defence companies to develop "backdoors" in products that increase the NSA's chances of obtaining information. Such "backdoor" measures undermine confidence in American companies. These days none of them can expect to be believed when they say their products are secure[4].

[2] One example could be the transfer of Oliver Hazard Perry-class FFG-9 and FFG-11 frigates to the Polish Navy in the years 1999–2000.

[3] State security services usually work in close cooperation with the Ministry of National Defence to ensure that the tactical communications system of the Armed Forces of the Republic of Poland offers proper and strong cryptographic protection.

[4] Covertly weakening the security of the entire internet to make snooping easier is a bad idea, p. 14; The damage the spooks are doing, p. 65; Is it possible to build a secure backdoor? Maybe, p. 67; The Economist, 14.09.2013.

The conclusion is as follows – other countries' tactical communications systems and cryptographic protection devices should not and must not be trusted, unless national cryptography is applied in a controlled manner. Everyone hopes they are the last person to come into contact with the device and that the device is designed to make forced national cryptography 100% effective, rendering it inappropriate to hide software functions designed for interception (if the device ought to have such functions).

All new tactical communications systems must be designed with this cryptographic policy in mind. The Armed Forces of the Republic of Poland must be provided with the strongest, most advanced cryptographic technologies and must be able to ensure that the state has complete control over their implementation.

Rough Specifications For A New Tactical Communications System

The new generation of standard tactical radio transceiver for communications systems, operated by a soldier in a network-centric environment on the modern battlefield, will be a personal (handheld) and vehicular radio[5], a device that acts as a tactical:

- telephone with a PTT button and a headset for the soldier;
- soldier and combat vehicle data terminal;
- soldier and combat vehicle sensor hub, e.g. transmitting video or images;
- GPS and receiver of information from higher tactical levels (e.g., company, battalion, brigade);
- node in the combat network;
- module – a cryptographic protection device with appropriate encryption capability.

[5] The C4I subsystem must consist of a single soldier's personal radio and a vehicular radio (e.g. for KTO Rosomak and BWP-1). Both must be fully compatible in terms of the functionality and communications system and well prepared for the tactical and operational conditions on the modern network-centric battlefield and for the changing climatic (geographic) conditions in the area where they will be used by the troops.

One can think of a new tactical communications system as a kind of terminal or telephone equipped with an appropriate national cryptographic protection device.

The requirements for the new tactical communications system should be as follows:

1. Multi-band communications system supporting VHF and UHF frequencies (30–512 Mhz).

2. Designed in line with NATO standards.

3. Very strong built-in national or NATO cryptographic solution.

4. Access control system ensuring possibility of activation only by an authorized operator and protection against interception and use by an unauthorized person (no possibility of penetration by the enemy in the event of theft or loss).

5. System equipped with a mechanism of emergency deletion of cryptographic data and documents.

6. Good range properties of the system.

7. Easy integration with combat vehicles (e.g. wheeled armoured carriers, tanks) in order to integrate support for combat operations on the modern battlefield.

8. World-class advanced tactical communications technology in all subsystems.

9. Flexible system for future concepts of tactical communications and cryptographic protection.

10. Well-known and reliable sub-suppliers of electronic components.

11. Manufactured in Poland.

12. Thought-out schedule of repairs, spare parts and tests to ensure the proper functioning of the system.

Features Of The New Tactical Radio

A tactical radio should be designed to provide soldiers with an individual means of communication at the team – platoon level and integrated with the ICT system of the combat platform (e.g. KTO ROSOMAK, BWP-1).

Below are listed the main assumptions as well as tactical and technical parameters for a new tactical radio to be included in the communications system in the era of cyberterrorism:

1. Transmission of speech, data, images, and video.
2. Supports VHF and UHF frequencies (30–512 Mhz).
3. Supports narrowband and broadband networks.
4. Advanced radio functions.
5. Transmission coded with an embedded COMSEC module with appropriate encryption capability.
6. Cryptographic keys changed by radio.
7. At 1W power range of about 1200 m in an open area.
8. Resistance to intentional disruptions and cyber-attacks.
9. Operational in extreme terrain.
10. Interoperability within NATO.
11. Software-defined and able to support previous operating modes of tactical communications systems.
12. Diverse and advanced user interfaces:
    1. traditional PTT button and a hands-free option;
    2. voice activated menu;
    3. smartphone-like, app-based.

Conclusions

All new tactical communications systems must be designed in line with the national cryptographic policy. The Armed Forces must be provided with the strongest, most advanced cryptographic devices and technologies (e.g. the newest and strongest pseudo-random and asymmetric generators, public key systems for dynamic key exchange at the tactical level) and must be able to ensure complete national control over their implementation.

The new tactical communications system should perform all the desired functions in a manner that is controlled and easy to use, install and administer within the communications system of the Armed Forces of the Republic of Poland. Effective protection of the new tactical communications system against cyber-war, guaranteed by a strong national or NATO cryptographic standard and national control over cryptographic keys, protocols and algorithms, will ensure the reliability of the system on the modern network-centric battlefield. We must realise that a modern and reliable tactical communications system is a well-thought-out defence on the modern battlefield.

References:

Wireless Module WM 600 Operator Manual and Wireless Module SR 600 Operator Manual, Kongsberg ASA, Norway, 16.01.2010.

Tactical Software Defined Radio THOR, Kongsberg, Norway, 20.12.2018.

The Economist, 14.09.2013.

Poradnik dowódcy plutonu, Dowództwo Wojsk Lądowych, Warszawa 2011.

WZTT na System Zarządzania Walką Szczebla Batalionu KTO ROSOMAK BMS i ZISW TYTAN.

Regulamin działań taktycznych pododdziałów wojsk pancernych i zmechanizowanych (pluton – kompania – batalion), Dowództwo Wojsk Lądowych, Warszawa 2008.