Strategos, 6(2), 2022, 177-206
UDK 32
UDK 355/359
Professional paper

STRATEGOS

Improving the integrity of military-defence communication systems using network access points with a focus on terrestrial radio-relay links

Tomislav Kravaica

Abstract

Obvious changes in a very broad field of the information and communication technologies are the key driver of the accelerated development of every sphere of human activity, including private life. In the military organization, this technological progress is present through the "post 2000" concept of the networked implementation of operations, which is implemented to varying degrees in armies around the world. New confrontations on the modern front include demands for an ever-increasing volume of the electronic traffic, complexity of the systems that generate, share and consume information content, and above all, the fastest possible availability of the relevant information. The race for information superiority is accompanied, on the other hand, by an ever more destructive highly sophisticated threats, from classic degradations and physical destruction, action of the hybrid (intelligence-combat) platforms of the unmanned systems, to cyber-electromagnetic activities of an offensive-defensive nature.

The new paradigms of the multi-domain warfare and expected scenarios that such forms of engagement put forward, demand from the modern military organization further normative arrangements within the functional area related to communication information systems. At the operational-strategic level, they imply the introduction of adequate organizational concepts and doctrines, while in the implementation part they require correction of the established tactics, techniques and procedures.

In such an operational environment, integrative efforts within today's military-defence communication systems transformed into unique complete solutions have brought a special challenge. Key networking of the mission components is provided by network access points. For this reason, they are the subject of special attention of the network designers, both conceptually and in terms of implementation. The effectiveness of their functioning is also an assessment of the maturity of military thinking, inventiveness and engineering practice – which will bring along defeats or victories to any combat system in future challenges.

Keywords

tactical communication system of land combat forces, military-defence network of strategic level, integrity of military-defence networks, network access point, deployable communication and information system, MANET network, terrestrial radio relay link, multi-domain warfare

Introduction

In the entirety of the military-defence electronic infrastructure, tactical communications networks (TACOMS) of the land combat forces (LCF) consist of the communication networking systems of modular forces that operate in the land part of a certain area. In the context of NATO terminology (NATO MC337, 1994), LCF primarily refers to the Army (KoV) and the existing ground facilities[1] of other branch components. These networks are joined by communication channels of joint action - according to the superior multi-branch command structure, and support elements from the Air force, Navy[2], special and amphibious forces. TACOMS is designed as a means of directly supporting the combat function of command and control (C2) within corps-level forces. In order to meet the requirement of frequent

1 Ground installations mainly include barracks, command posts, airports, helipads and airfields, as well as aerial surveillance and guidance radar positions, naval bases, ports, moorings and naval coastal surveillance positions, logistics and accommodation bases, and military training grounds.

2 In the littoral area of shallow and narrow seas such as the Adriatic, the Baltic, etc.

movements, TACOMS elements are required to have extremely short setup/disassembly times – usually within several hours (ATIS Telecom Glossary, 2019). Its individual entities are created depending on the user's operational requirements – grouped into series of influential persistent and variable factors[3] (NATO C3B, 2008).

In the paper, the author presents a systemic and organizational-technical view of possible solutions for continuation of development of the next-generation tactical communication networks of the LCF. The context of the paper is oriented towards reflections on the integrity of the dynamic TACOMS – firmly based on the statically oriented military-defence network of the strategic level – which, united in this way, form a compact functional unit. The guiding principle of such a point of view is focused on adoption of new concepts, continuation of national acceptance of the acceptable NATO standardization agreements (STANAGs), as well as development of the existing doctrines. At the same time, it is an obvious way to improve mutual understanding, that is, to increase the level of interoperability within components that strive to act synergistically in a multinational environment.

The source of this approach is primarily doctrinal commitment of the Croatian state policy to a defensive way of using its Armed Forces (GSOSRH ZDP-1(A), 2016), along with active participation in collective defence systems – such as the North Atlantic Treaty Organization (NATO) and within the European Union (EU), and engagements within the peacekeeping forces of the United Nations (UN).

Due to universality of the military concepts at the operational-tactical level - mainly due to the trend of global acceptance of today's and upcoming technical-technological solutions, the content of the paper does not have to be exclusively related to the Croatian Armed Forces, but is acceptable to other similar armies in the world due to its equivalence. For this reason,

3 Persistent: according to the type (man, vehicle, aircraft, tent, container), operational area (land, air, sea, submarine), degree of mobility (action in stop, in motion, in fast movement) of the platform. Variable: through connectivity, connection length, i.e. platform density, electromagnetic environment, i.e. threats related to electronic warfare – including cyber threats, and required traffic capacity.

as an example everyone can relate to, in the second part of the paper, implementation of the network interconnection using a terrestrial radio relay access point is methodologically elaborated.

Integrity of the military-defence communication networks

Land combat force TACOMS rely on strategic-level networks (Ryan&Frater, 2002) – encompassing the entire state structure, including permanent military-territorial deployment. Due to stationary nature of the permanent accommodation, this General-Purpose Segment (GPS) of the military networks is related to the long-lived static/fixed part (NC3 IO-HB/EO, 2008) of the defence infrastructure. This primarily refers to permanent locations of the military forces in peacetime – which, due to their daily functioning, are permanently connected by a core network of the market-provided telecommunications capacities and guaranteed service levels (SLA – Service Level Agreement). It is a continuously built national critical infrastructure (NATO MC337, 1994)[4], whose integral part consists of the communication centres (COMMCEN) regional, nodal, access levels – located in security-technically appropriate conditions that ensure solid buildings.

Contemporary TACOMS are activated during military operations in the multi-domain battle space[5] environment based on current usage doctrines

4 According to the "Act on Critical Infrastructures of the Republic of Croatia" (*Official Gazette* no. 56/13, 2013), communication and information technology is considered very important in the organization of the national critical infrastructure, due to its direct connection to state administration bodies, including its military and defense sector. In this context, its protection is related to ensuring the functionality, continuous operation and delivery of services/goods of critical infrastructure and preventing its endangerment. Depending on the nature of security threats, GPS can be additionally treated through a Special Purpose Segment (SPS) to support military operations that monitor specific, for example, nuclear threats (NC3 IO-HB/EO, 2008).

5 „This concept advances the proven idea of combined arms into the 21st-century operational environment by describing how future ground combat forces working as part of joint, interorganizational and multinational teams will provide commanders the multiple options across all domains that are required to deter and defeat highly capable peer enemies. Multi-Domain Battle requires flexible and resilient ground formations that project combat power from land into other domains to enable joint force freedom of action, as well as seize

(NATO STANAG 2525, 2017). They are in operational work as long as there is a need for it – ensuring the capacity of sufficient and operationally reliable communication channels necessary for information flows within the command and control system (C2S). As a support element, they are formed in accordance with the operational requirements and force structure in a given battle space[6], in a certain chronological time and meteorological weather, with clearly defined objectives within the assigned mission.

According to the degree of mobility, TACOMS consists of two main parts: deployable – with a feature of communication within the headquarters of the forces in halt (CATH – Communications At-The-Halt) – also related to fixed locations, but of temporary importance (important while the operation lasts), and the moving part – related to the communication of individuals, teams or manoeuvre forces, as well as their supporting elements in movement (COTM – Communications On-The-Move)[7].

Based on lessons learned from "post 2000" military operations – especially ISAF (International Security Assistance Force) in Afghanistan (NATO TACOMS ISAF, 2010), integrity of the military-defence communication networks close to the NNEC (English NATO Network Enabled Capability) concept (NNEC FS-ES, 2005) is formed of three indivisible parts: a static part – which also constitutes the strategic level, and the tactical level – which consists of the deployable and mobile components (Figure 1a).

positions of relative advantage and control key terrain to consolidate gains." (General David G. Perkins, USA, 2016, the then commander of the TRADOC Command of the US Army – source: https://www.ausa.org/articles/multi-domain-battle-joint-combined-arms).

6 In the context of land combat operations, the term "battlefield" implies a physical three-dimensional battlefield, related to the land, coast and air, as well as virtual cyberspace closely related to the electromagnetic spectrum.

7 In the USAF, TACOMS implementation is carried out within the framework of the WIN-T (Warfighter Information Network-Tactical) program through several steps of increasing capabilities. The first step, which implied CATH capability was initiated during operations "Iraqi Freedom" and "Enduring Freedom" in 2004 and concluded in 2012 with the equipping of the U.S.Army, National Guard and reserve forces, while the second involves COTM capability – started in 2013 in Afghanistan (USA ATP 6-02.71, 2019 / FMI 6-02.45, 2009) (source: https://gdmissionsystems.com/communications/warfighter-information-network-tactical), accessed 06.04.2022)

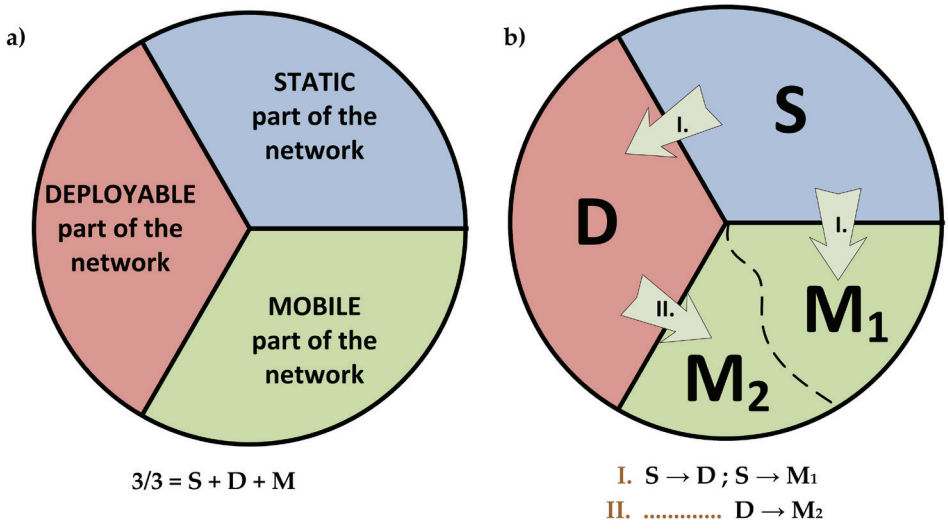

Figure 1. The integrity of the national military-defence communication infrastructure through the "S-D-M concept" (a), with ways of operational growth (b)

The unique integrity of defence-military networks is manifested by systematic provision of the "end-to-end" communication and information services, regardless of the category of mobility of a particular segment of the system (NATO MC0593/1, 2014). This implies a fully interoperable connection of network entities, faultless traffic flows (NC3 IO-HB/EO, 2008), including security aspects[8] of the communication and information system (CIS).

In tune with the network centric operations (NCOs) paradigm, the technical feasibility of the "S-D-M concept" (or "3in1" or "3/3") was achieved by maturation of a series of technological solutions that gradually entered military application – often from the consumer goods market. Conceived in the mid-90s of the 20th century, it was realized through digitization by the end of the decade, while it experienced full affirmation in the first years of the new millennium – in the NATO alliance through the "TACOMS

8 "Security aspects" mainly mean adequate separation of security domains of classified networks and a single compatible policy of cryptographic protection of communication paths.

Post 2000" set of normative agreements (NATO STANAG 4637, 2010). While this outline in its first phase (2009-2014) included the use of legacy military (EUROCOM) and civil (ITU) telecommunication standards[9] that were difficult to reconcile at that time – with gradual introduction of the ultra-wide internet technology, the second phase "TACOMS Post 2000" (2013-2018) was exclusively based on closed intranet networks with multi-level IP (internet protocols) protocol composition (NATO C3B, 2009). Today, in military organizations, this is largely achieved by unique multi-service digital communication platforms, based on packet transmission of information content, Internet technology, and wireless software-defined[10] connection with advanced modulation procedures (Poularakis, Iosifidis & Tassiulas, 2018), thus allowing convergence of the networks and services, with multifunctionality transport or portable user terminals installed in various mobile combat platforms (Figure 2) of the manned or unmanned type – the networked Internet of Things (IoT).

The advantages of such a complementary design of military communication systems point to the optimal use of the available network resources of the state defence system – which is visible through a number of aspects, the most important of which are:

- in operational meaning, it very quickly goes from peacetime to crisis (crisis response operations) or war (combat operations), including military engagement in humanitarian operations (operations to support civil institutions)[11];

9 NATO STANAG 4578 The NATO multi-Channel Digital Strategic-Tactical Gateway (DSTG), edition 1, 2003 / Enhanced Digital Strategic Tactical Gateway (EDSTG), edition 2, 2009.

10 Software Defined Radio (SDR) – contemporary versions of digital radio systems in which the functions of traditional hardware components are replaced by software using computer technology. This approach, established in communications, implies radio frequency (RF) circuitry with a series of protocols related to waveforms changing in real time. Some of the SDR techniques are spread spectrum and ultrawideband, software defined antennas, cognitive radio, wireless mesh network, frequency escape, automatic transmit oower control, side lobe cancellation and near-far problem, etc.

11 Types of operations according to the NATO doctrine AJP-01(E), accepted in allied operations through ZDP-1A.

- safe manoeuvring is achieved through connecting roads, especially over long distances, where the established strategic backbone – with significantly better traffic and technical performance serves to interconnect individual enclaves of the deployable communication network, without limiting its spatial-physical compactness during expansion;
- the use of detours, i.e. alternative connecting routes between any two points on the front line, contributes to greater network availability;
- shortening the preparation of the establishment of communication channels of the growing network;
- easier connection with various structures both in the country and between the allied forces – important for the accomplishment of the mission;
- safe mutual support in case of major losses in the network infrastructure, especially the moving elements of TACOMS.

The dynamics and sequence of growth of the integral military-defence network (Figure 1a) will depend on the potential of available resources, and nature of the escalation of the operation: from static (S) to deployable (D) (I.), and then to mobile (M_2)(II.) or by simultaneous growth (I.) from static (S) to deployable (D) and mobile (M_1).

The extent of TACOMS engagement during a military operation – with its deployable and mobile effects will depend on the required degree of mobility and spatial dispersion of C2S, combat and sensor platforms, and elements of combat protection and support, as well as the development of the static part of the infrastructure.

Network access points

According to the "post 2000" military standards (NATO STANAG 4637, 2010), a wide area network (WAN) as a special subsystem of TACOMS connects immobile groups of users via a backbone of wireless links of high transmission capacity. This ensures the necessary flow of information from front units in direct contact with the enemy, along the line of subordination to the highest command (Echols & Lysek, 2006).

In this regard, an integral part of CIS planning is assessment of the needs for the establishment, first of all, of the broadband/high capacity duplex network access points (NAP)[12] (Figure 3):

- connecting the static and deployable part of the military network (SDAP) ensuring network points of presence (PoP) according to groups of users in dislocated locations, and "ad hoc" activation of intervention (primary or secondary "backup") links between more permanent (so-called garrison) headquarters of commands and units,
- field connection within the coverage zone (point-to-zone communication) of the battlefield MANET (eng. Mobile Ad-hoc Network)[13] radio networks with tactical regional backbone (RAP from radio access point) (USA ATP 6-02.71, 2019).

NAPs are boundary elements connecting static and deployable, deployable and mobile, and if necessary, static and mobile[14] part of the military-defence communication networks (NNEC FS-ES, 2005) (Figure 2). For this reason, they are at the same time critical places in the network where different technical solutions and opportunities for mutual interaction are exchanged[15], security classified network domains[16], as well as the chronologically increasing stability of system functioning.

Here, a tactical part of the network is connected to the already established fixed infrastructure, which upon activation begins to function in a challenging, highly demanding and destructive hostile environment.

12 The US Army and Marine Corps within LandWarNet have been using STEPs (standardized tactical entry points) (USA FMI 6-02.45, 2007 / US MCWP 6-22, 1998).

13 The battlefield MANET of the broadband tactical communication system implies the creation and establishment of a network backbone between its clusters of the network – through cluster heads.

14 Mobile networks of regional, national or global coverage – security adapted to military needs.

15 Interoperability means the technical dimension of communication interoperability between connected network entities.

16 Security domains imply strictly defined degrees of secrecy of data that can be transmitted and processed within a certain classified CIS. They are observed in the national and coalition environment.

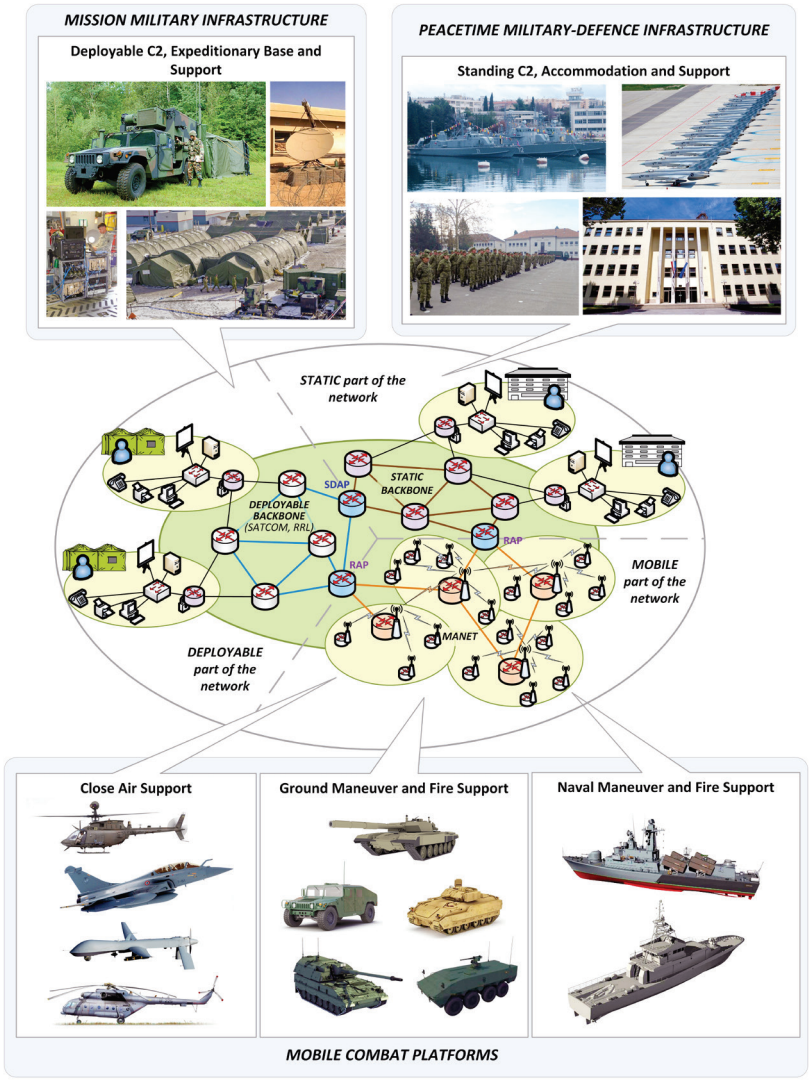

Figure 2. Integration of the defence static communication network with deployable area extension and mobile combat platforms[17]

17 In practice of the real battle field – in addition to combat, sensor and (combat) support platforms are used.

With technical support of the wireless means of communication, military-defence networks make a step forward to the stage of electronic warfare, and considering the uniquely accepted Internet platform – and the complicating set of threats brought by cyber warfare. This is all the more reason for the existence of the functionality of monitoring their condition through the system of existing centres for management and monitoring of the network (NATO, RTO-TR-IST-067, 2010)[18].

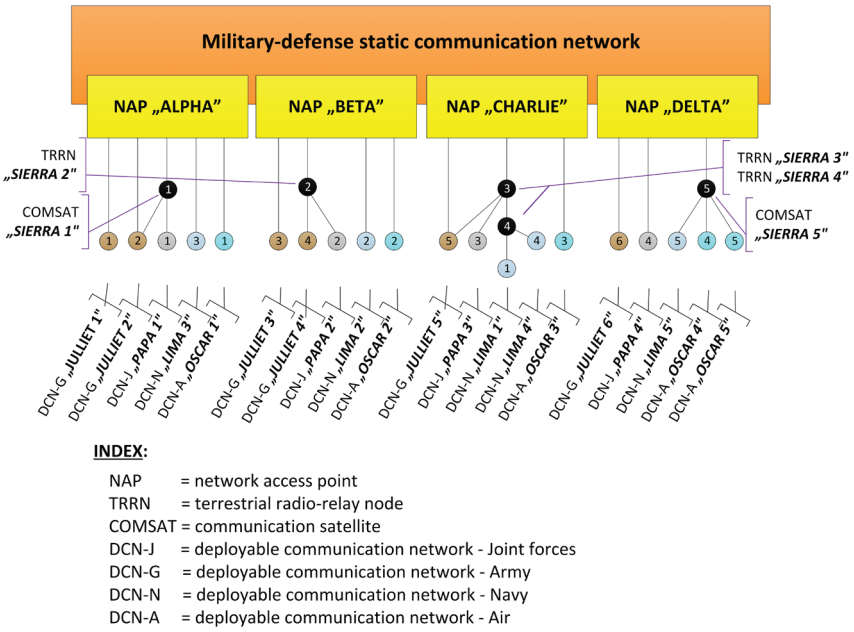

Figure 3. Extensions and spatial extensions of the military-defence communication network via network access points

18 In the case of more complex communication systems, centers for managing and monitoring the network, including their connecting access points, can be hierarchically organized into main regional/district access centers (DAC) – which can be primary (PAC) and secondary (SAC), nodal and local – minor (MAC) access centers) or end user – terminal access centers (TAC), with assigned responsibilities. In the static part of the network, they are permanent, while tactical ones are of temporary importance (from the reference document: Annex D – Network Evolution Under NNEC Concepts – Technical Study, Selex Communications A Finmeccanica Company, 2007, pp. D38/39).

The method of performing NAP is achievable through established systematization of several available transmission solutions (Figure 3): using terrestrial radio relay (RR-AP), radio troposcatter (TROPO-AP) and satellite (SATKOM-AP), with increasing military implementation of the originally commercial wireless solutions (for example WiFi and WiMAX). While radio relay, WiFi and WiMAX NAPs are used for development of the networks at distances within the line of sight (LOS), financially more generous radio troposcaters and satellites are used for the establishment of connecting links at greater distances. These are connections beyond the line of sight (BLOS – from Beyond Line of Sight) – when the use of terrestrial radio systems is not feasible for some reason.

Depending on the connection method, several NAP radio solutions are available, so the following are possible:

- terrestrial radio relay access points – one or more end radio relay stations – to which spatially distributed tactical intermediate stations, nodes and end stations are further connected;
- satellite access points – with a hub station of a "corporate"[19] star topology towards one or more spoke stations within remote enclaves;
- radio troposcatter access points – with which, thanks to the tropospheric scattering phenomenon, radio links significantly longer than terrestrial radio relay ones (up to 400 kilometres) are realized;
- MANET radio access points – where you switch from a static, i.e. deployable, mode of communication – to a mobile one.

Elements of the network access point

The elements of the network access point, in a broader sense, consist of: radio transmission and switching-routing, crypto-protection equipment with accompanying infrastructure, assigned radio frequencies, and personnel who serve the system according to prescribed standard operating procedures (SOPs) related to operation, maintenance, supervision and management, and system protection.

19 Connecting headquarters with branches via satellite, according to the most economical "star" topology.

Radio communication equipment is an essential element of the NAP. It is intended for adjusting the procession of digital impulses (bit/s), and through an antenna of appropriate direction – for free space transmission in the form of modulated high-frequency signals, i.e. with a simultaneous reversible process for receiving, demodulating and processing signals in the opposite direction. Its set composition is configured in the form of a wireless network interface – specified communication protocols, access methods, network numbers and addresses. Duplex digital communication traffic of high transmission capacity is carried out depending on the network topology – to one ("point-to-point") or several ("point-to-multipoint") opposite ends of the links, i.e. to a group of users in space ("point-to-zones"). In addition, the external RF unit consists of the interfaces to which the internal unit is connected with switching-routing devices and crypto equipment.

As a rule, the accompanying electronic communication infrastructure intended to ensure the functioning conditions of the MPT consists of the following elements (Figure 4):

- fixed antenna pole, in more complex cases an antenna tower or caponier[20] (A) within the antenna farm (AF),
- enclosed space (container, tent, solid object, dugout) in the form of a shelter, for housing and creating working conditions for communication equipment (S),
- local communication centre with network equipment (COMMCEN),
- local cabling and fibre optic infrastructure (underground pipes and wells) which enables RF dislocation (LCI),
- energy block with power sources (E),
- safety-protective fence (F) and equipment.

If the requirements so dictate, a suitable fixed or prefabricated antenna pole or tower is placed on the location, the structural complexity and height

20 Antenna caponiers are reinforced concrete buildings in which microwave radio relay antennas are installed. They are partially or completely covered with special covers, which serve to protect against meteorological and climatic influences, as well as a covert element. In the interior of the caponier, there is a pipe support to which a microwave antenna with directional radiation is attached, a pipe sewer with an antenna cable, and a grounding strip.

of which are determined based on features of the radio equipment used, geographical conditions, and the target area of radio coverage from the position of the NAPs[21] a special, but not rare, case of placing antennas on roofs, terraces, balconies or walls of buildings. Such solutions facilitate the placement and interconnection of elements: from ensuring a sufficient height of the antenna, to a room for the placement of radio communication and network equipment, domestic sewage inside the building, power sources, living and working conditions of the staff, ease of manipulation with the equipment, better safety and protection measures and the like.

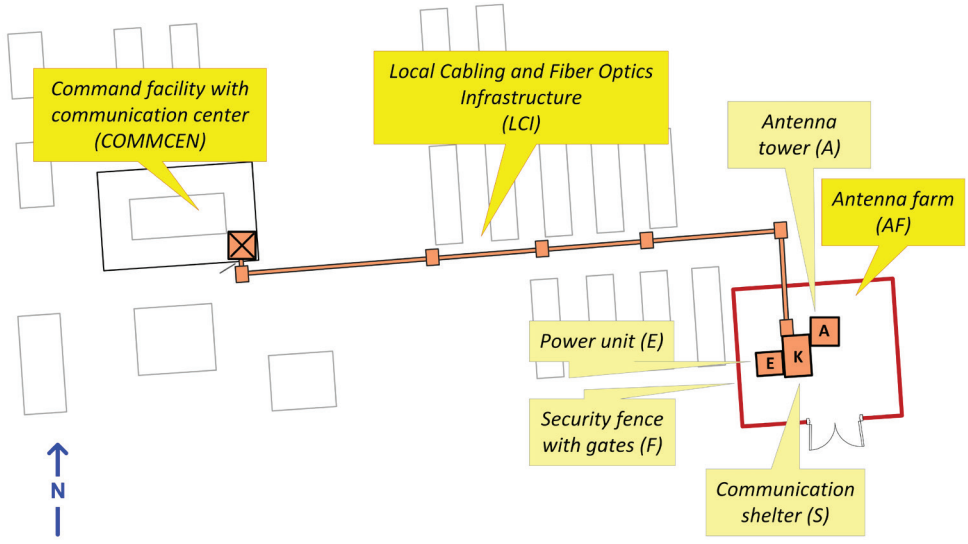

Figure 4. Arrangement of the radio relay access point elements within a permanent military location

At the place of installation, it is necessary to arrange the terrain with a series of adequate construction interventions, through:

- preparation of the working surface (soil, concrete slabs, filling of stone/gravel of larger granulation) – which ensures the drainage of

21 Command post survivability factors are taken into account – mainly dispersion, reflection and camouflage.

rainwater, movement and manipulation, and creates the conditions for adequate fire protection (formation of a fire belt),

- ensuring access space for movement and manipulation of the container (delivery/removal, lowering/lifting from/onto the vehicle), including appropriate doors on the protective fence,
- connection of the container to the electrical network with the possibility of using an electrical generator,
- feeding and connecting the container to the local communication sewer and further to the top of the pole, that is, to the platform intended for installation of antennas.

For placement of the radio communication equipment, it is necessary to provide an enclosed space in which climatic conditions have been created for its proper operation[22]. In the most common cases, it can be a suitable room in a solid object with a certain degree of protection[23] or a typical communication container that is placed right next to the antenna pole. The container can be of commercial design or, in the military sense, a more practical solution[24] – a tactical communication cabin removed from the vehicle.

Individual, spatially separated parts of a set of radio devices and network equipment in the relationship: "antenna pole – connection container – local communication centre" are connected to each other by cables, most often through underground local distribution sewers.

22 Regardless of the design, such enclosed spaces contain: multi-option automatically regulated electrical power installation, heating/air conditioning system, adequate lighting, and appropriate equipment for working on the antenna pole.

23 The types of construction facilities for the accommodation of COMMCEN range from unfortified above-ground, underground fortified, to above-ground-underground. For security reasons, the national regulations with applied measures in this area for each country are limitedly available, that is, classified. In accordance with special norms of resistance to nuclear shock, with thermal, radiation, chemical and impact effects - underground versions of the buildings were built for living and working conditions, which ensure the SPS category of critical KI infrastructure.

24 For these reasons, available TACOMS cabins are often used in military practice - given that they already have a purpose-built and certified power installation, heating and air conditioning systems, as well as adequate lighting - according to NATO standard ACE 6516/ SHCPE/86 - Standard Shelter Technical Specifications, Allied Command Europe, 1986.

Safety and security measures at the antenna pole construction site are applied in accordance with legal regulations prescribed for this type of facility, through:

- protection of the antenna pole/tower from atmospheric influences (corrosion),
- fencing off the space around the pole by installing a safety-protective fence, in order to prevent unauthorized access, as well as to protect personnel from objects falling from a height,
- installation of the grounding system for the pole and the cabin, as well as lightning protection installations,
- prescribed marking of the pole by painting and installation of light signalling[25],
- installation of physical protection measures (fences) for personnel moving along the tower during work (on stairs/ladders) and on its platforms,
- application of prescribed fire protection measures,
- installation of suitable external lighting for smooth operation at night,
- installation of a video surveillance system, i.e. notification (alarm),
- setting the necessary warning signs.

Finally, in accordance with general regulations, the antenna tower with the accompanying infrastructure must be certified and periodically technically inspected by authorized certifiers.

When choosing a place to install antennas on a building (roof, sidewall or balcony/terrace), safety and security conditions must be observed, such as ensuring unhindered access to the flue and air conditioning system, as well as devices located on the roof, including the electrical installation.

Antennas of the radio devices must be placed in such a way that their radiation cannot negatively affect people's health.[26] This is especially important when

25 Defined by ICAO norm: "International Standards and Recommended Practices, Annex 14 to the Convention on International Civil Aviation, Volume I – Aerodrome Design and Operations", ed.5, 2009.

26 For terrestrial radio relay systems, professional exposure should be distinguished from

installing antennas near open areas of human habitation. Such dangerous influences need to be adequately neutralized by sufficiently raising them to an acceptable height, and by properly directing the radiating elements "outward" into free space.

Placement of the network access points in the space

Military locations for installation of the NAP are not mere places of public telecommunications infrastructure, but strategically planned (NATO SOCJ6/121/02, 2002), systematically selected, organizationally well-designed, self-sufficient technically capacitated and adequately protected signal sites that must meet appropriate tactical, technical and support conditions.

Tactical factors such as spatial distribution of the positions of own (combat support directions) and opposing forces (directions of possible threat), applicable measures and procedures of concealment and defence in static conditions can be considered in the situation of peacetime functioning, various crisis situations and in conditions of threat due to combat enemy action.[27] In the area of one's own sovereign state territory, the position and distance of the selected location from the border with the neighbouring country, its allied status in the system of multinational collective defence, measures to conceal location of the NAP, the method and organization of active and passive defence, including counter-electronic protection measures[28], are generally

civilian exposure. Personnel exposure to electric and magnetic fields is defined by standard C18-610/ENV 50166-2 (high frequencies/10 kHz – 300 GHz, January 1995), which sets a safety threshold of 5 mW/cm^2 at a frequency of 5 GHz. The safety threshold for the civilian population is five times lower and amounts to 1 mW/cm^2.

27 The issue of security and protection zones around military facilities in the Republic of Croatia is defined by a series of regulatory documents, such as the "Regulations on the method of securing military locations and buildings particularly important for defence" (MORH, 2014) and the "Regulations on protection and security zones of military facilities". (MORH, 2003).

28 When considering the distance and direction of the NAP in relation to the state border, it should be determined whether the direction coincides with the direction of a potential radio relay link (possibility of "breaking into the link" and eavesdropping from the neighbouring

considered, as well as an appropriate degree of engineering arrangement and applied protection against physical vulnerability.

In mission environment of the expeditionary forces in the area of operation, safe zones (perimeters) are limited to the space within well-guarded bases/camps. In this case, it is important to consider possible influence of the adversary's threat on the functioning of the NAP from the intermediate space between military installations.

It is very difficult to hide the location of a military installation, both peacetime and expeditionary, especially when it comes to fixed infrastructure. COMMCENs, and especially easily visible antenna installations (by visual observation and radio reflection), are often targets of the first wave of fire by opposing forces (air force, artillery-missile action, drones, etc.) or special forms of action such as diversions or terrorist attacks. For this reason, it is appropriate to move the poles with installed antennas as far as possible from the command posts, which include the COMMCENs themselves (visible in the example shown in Figure 4).

Facilities for accommodation of the personnel and equipment for this part of the military infrastructure are built (in whole or in part) below ground level. For buildings like this, special construction measures are applied – in accordance with estimates of the destructive power of potential weapons. Today, the most common practice is that, if legacy military infrastructure is not used, NAP elements are placed entirely or partially above ground level, with certain degrees of ballistic protection by engineering fortification.

Factors such as geographical features of the location, terrestrial radio relay routes, influence of the vegetation, alignment of directional antennas, future intentions in development of the network, radio coverage of the surrounding area, RF interference speak about technical point of view of the NAP, i.e. placement of the military radio communication equipment pertaining to technical specifications.

territory) or general circular radio broadcasts. For this reason, when planning, designing and installing equipment, it is necessary to apply countermeasures to the influence of possible electronic activity. With satellite and tropo links it is less important.

It is difficult to change a natural basis[29] of the environment for conducting military operations. It is determined by geographical features, degree and methods of construction (urban environment), existing vegetation in immediate and distant surroundings of the location, and the relief itself – which influence the spread of the surface terrestrial component of electromagnetic waves, especially on routes interesting for the establishment of directional radio links – the so-called radio relay corridors. However, selection of the most favourable micro location within the existing military installation in relation to known parameters, especially antennas and devices, the position of other electronic equipment and power installations that could affect functioning of the NAP (RF interference) is the key to ensuring, not only the establishment of directed radio links to remote locations, but also ensuring radio coverage in the area for the most favourable development of the tactical communication network.

It is necessary to identify all negative protrusions in the relief, the influence of vegetation, water surfaces, larger buildings, and power installations (substations, transmission lines) that can affect the quality of the wireless link or can be found as an obstacle that creates a "radio shadow" for establishing a connection to some parts of the surrounding area.

For this reason, after computer simulation of the radio propagation and survey, it is proposed to install (or use the existing) fixed antenna support structure for placing antennas at the most favourable micro location in the barracks. This assesses whether holding the specified position will create the "best possible" conditions for connecting deployed or mobile users to the network access point (Figure 5).

This implies careful consideration of the directions for the most favourable radio communication openness from the location of the NAP, that is, the introduction of improvements – relying on existing or subsequently installed network nodes in the surrounding area.

29 In the context of the discussed topic, the natural basis refers to: relief, hydrography (sea, i.e. coasts, rivers, lakes), climate, plant cover (vegetation).

Factors related to physical access to the location are a supporting part of NAP functioning. They include routes for the supply of people, equipment, energy, food and beverages, as well as spare parts and technical maintenance. It is a complementary and no less important element in achieving the optimality of the choice of spatial arrangement of each NAP. In this sense, if the circumstances allow, NAPs can be formed at locations of the static military communication infrastructure – due to a number of advantages that such places bring along. These are: existence of a permanent human crew, an already established logistics supply system and a security and protection system (on-call and guard service, technical supervision and protection) – as regular forms of functioning that do not require daily engagement of additional CIS personnel.

Plan-project elaboration

When connecting TACOMS – whether it is its deployable or mobile part to a static communication system, NAPs are placed in accordance with intention of future expansion of the overall network. For more permanent infrastructural solutions, operational plans are to be put forward that include all elements important for establishment and exploitation of one or more NAPs, and for the sake of expeditious activation – it is necessary to elaborate the project.

Depending on the design and applied connection solutions, the report documents the physical location and spatial arrangement of all elements necessary for the NAP to function, the configuration (set composition and software settings) of the equipment with their connection schemes and radio coverage in the surrounding area, openness to communication satellites as well as assigned radio frequencies. In order to avoid radio interference, it is desirable to be familiar with the situation in the electromagnetic spectrum at the location itself before making a final determination of the frequencies at which the radio communication equipment will work.

The project studies include results obtained by expert site survey, as well as recordings of the virtual simulations and calculations of the radio paths,

radio coverage achieved from the NAP, azimuths and elevations according to available satellites obtained using some of the available computer applications. Thus, in the context of recording the state of the surrounding relief of the land (with coastal area if the circumstances are such), the state of vegetation, built structures and resulting possibilities of the geospatial orientation (0-360°) azimuth and elevation (+/-°) of the directional antennas – the most favourable remote points are identified in the coverage area.

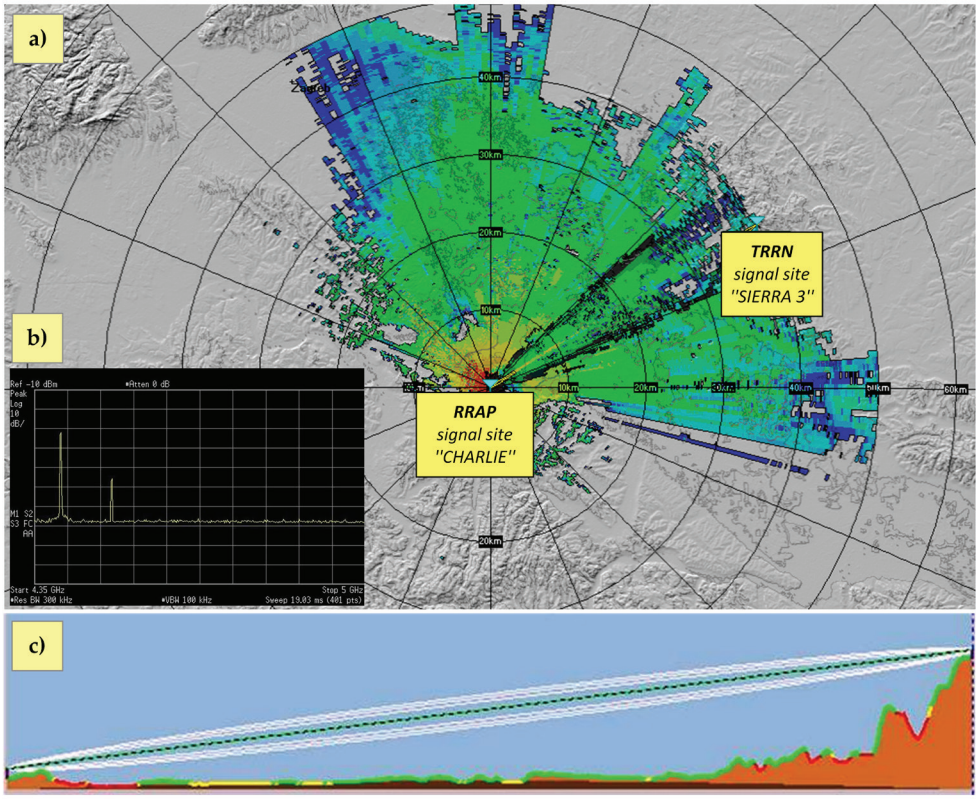

Figure 5. Radio coverage of the radio relay access point with a possibility of developing a deployable communication network via neighbouring radio relay node

Case study: Development of the radio relay access point

The preparation of NAPs as part of the activities of the military organization of the territory in individual locations depends on the encountered situation and the degree of targeted functionality of the military-defence communication infrastructure. As shown in Figure 6, solutions can range from adaptation of the existing electronic communication infrastructure (ECI) for a new purpose to a completely new construction intervention in the space. Investment cost is often a predominant factor, so in practice, among several possible NAP locations, the one that requires smaller financial investments is usually chosen.

Military practices show that despite efforts of systematic standardization, each individual NAP should be dedicated in a unique way. The reasons are in the real specific characteristics of each individual location – which require determined network performance. The most common differences can be related to composition and configuration of the equipment (complexity requirements), but also to the infrastructure part. For example, it can be about the practical implementation of the installation of antennas, dislocation and methods of local connection of the internal (indoor) and external (outdoor) RF block of the system, as well as the physical specific characteristics provided by the location itself.

The initial selection and further expansion of the NAPs on the territory of state sovereignty are the result of developed CIS support scenarios as part of the comprehensive military-defence plans (NATO SOCJ6/121/02, 2002). If it is about expeditionary action of the forces engaged in the area of operation outside the home state territory – the development of NAPs is carried out on basis of the overall CIS plans for development of the mission network (NC3 IO-HB/EO, 2008).

Connection of the radio relay and network equipment at the RRAP location within the military installation (barracks, bases, camps) is carried out after computer simulations[30] and field surveys, guided by operational-tactical and

30 Some of the most widespread planning and project tools for radio networks used in the NATO alliance are: the American SPEED (Systems Planning, Engineering and Evaluation

system requirements in terms of telecommunications of the network itself. The project task, elaborated through several versions, should be prompted by the expectations set for the NAP (purpose, place and role within the network). Opportunities can be created by stages in the construction (growth) stage of the communication functionalities of the RRAP – and there can be more of them. Such an approach, adopted in military engineering practice, may be the reason for gradual construction of the NAP through several stages: from mere ad-hoc tactical performance (initial communication functionality – Figure 6a), which can be functionally supplemented (Figure 6b), to the phase of use of a fortification-arranged solid structure (Figure 6c), whose functionalities can also be supplemented chronologically (Figure 6d).

In the military practice of RRAP development, it is most often about configurations made up of a combination of exclusively military equipment (MIL-STD) and commercially available equipment (COTS/Mil-COTS)[31] (Figure 7), where according to the "red-black outline". "Red/Black" concept) (US 9,401,920 B2, 2016) the networks of one or more security-classified domains are connected (Morrison et all, 2016).[32]

While greater resistance to difficult field conditions[33] (external RF units) is desirable for more exposed external parts of the equipment, this is not a crucial requirement for the internal part (deployable communication node).

Device) – a professional military tool for the analysis, planning and design of tactical radio networks and "Radio Mobile" – a tool originally created and still maintained by a private person, but very popular and accepted by many professionals – including in the military world.

31 COTS – commercially (available) off-the-shelf. In the military world, especially in the USA, the hybrid solution between military and commercial performance is called Mil-COTS.

32 **The "Red/Black" outline** (or architecture) is based on the strict separation of parts of military-defense networks using cryptographic systems - into parts where plain text information is transmitted/processed ("red signals") from parts with encrypted information ("black signals "). This is how military networks are classified, with "national secret", "national unclassified" or "restricted", "mission secret", "NATO secret".

33 MIL-STD-810E, Military Standard: Environmental Test Methods and Engineering Guidelines (1995)

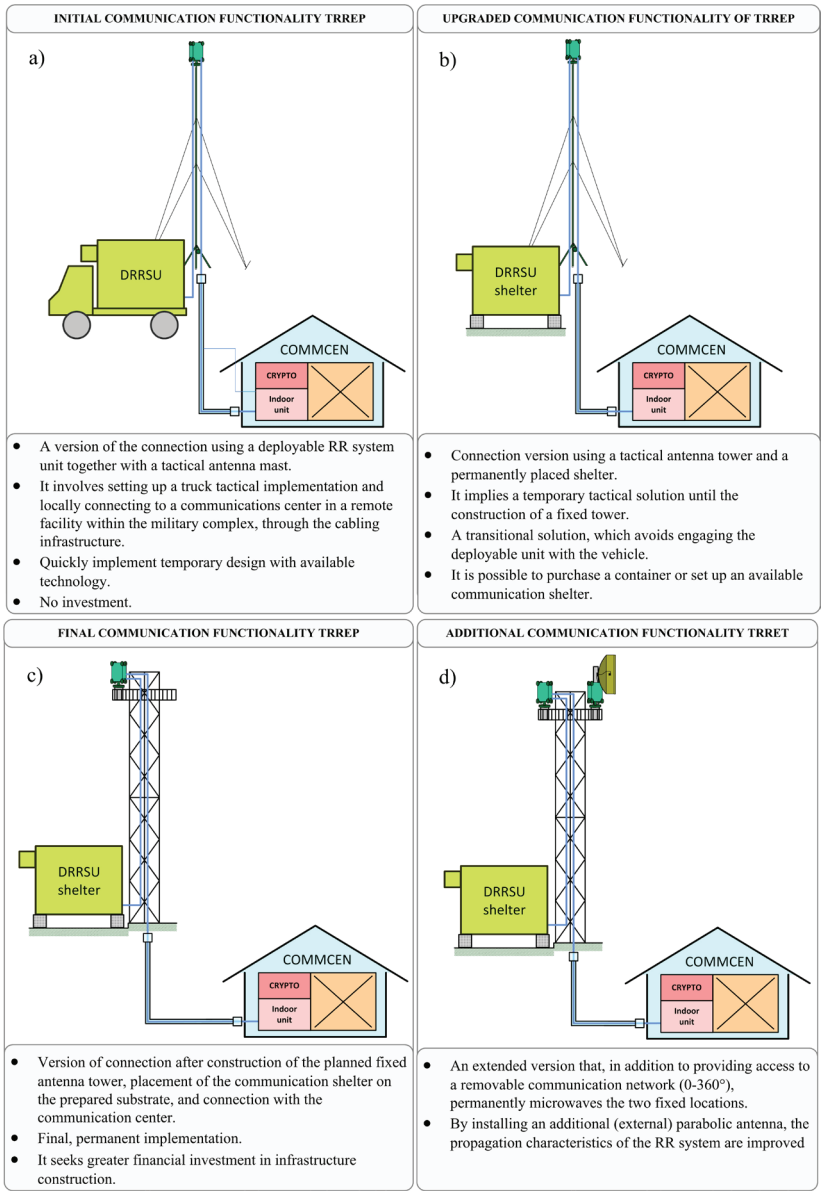

Figure 6. Phases of increasing communication functionality of the radio relay access point

Therefore, for the network part, equipment of commercial performance is often chosen, installed in possibly somewhat more robust communication boxes and cabinets. Final completeness of the composition of the kit that is placed on the NAP itself is not a decisive reference for a specific radio link, but rather it is tactical communication equipment that is installed in field conditions, at intermediate stations, nodes and at the end points of the network. For this reason, the consequent idea of adapting essentially tactical equipment to work in static conditions is understandable.

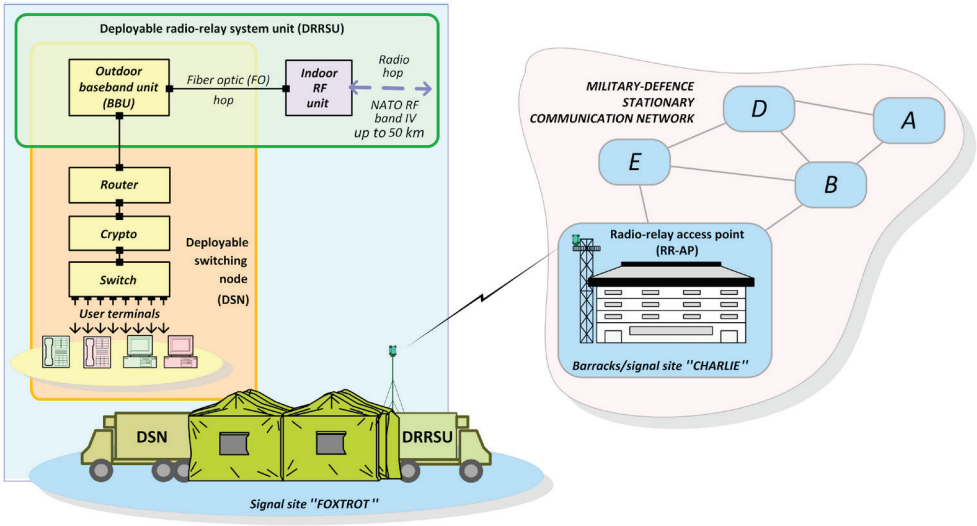

Figure 7. Tactical communication equipment connected to a radio relay access point

Conclusion

In the context of the upcoming TACOMS generation of complete integration, NAPs are the key connecting element of individual segments (static-deployable-mobile) of military-defence networks that differ categorically with regard to the degree of mobility. By jointly accepting the same information and communication technologies, primarily based on the Internet platform – for the first time, unified military solutions manifest the convergence of

end-user communication and information services – according to the "3in1" concept. Thus, from the highest commander to units engaged in direct contact with the conflicted adversary, the integrated TACOMS network combat, intelligence, and protection-support platforms, which do not necessarily have to have a human crew anymore but are manageable, with an increasing degree of autonomy.

Practically, NAPs can be different – depending on the characteristics of a particular military organization and a particular mission, the size of the area and environment of deployment, and the circumstances in which they are engaged. Methodologically, they are planned, designed, and installed with a comprehensive analysis of the tactical, technical and support factors. With elaboration presented through the case study of a terrestrial radio relay access point (expandable to other – even hybrid solutions of NAP), the paper expertly presented an example of a methodologically elaborated sequence, with possible optional increases in capabilities. In absence of a formal publication that deals with the discussed issue, the publication of this paper is an attempt to solve a very important organizational and technical issue that experts in the field of military-defence networks deal with, both in the Croatian Armed Forces and probably in other military organization around the world.

References

Alliance for Telecommunications Industry Solutions. (2019) *The ATIS Telecom Glossary*, ATIS-0100523.2019, Waashington DC, USA. *https://glossary.atis.org/using-the-atis-telecom* Accessed 12th May 2022

Echols, C. & Lysek, K. (2006) *Tactical Interoperable Communications Standards (TACOMS) – A Key Enabler to achieving NATO Network Enabled Capabilities*, TACOMS POST 2000, International Project Office, France.

The CAF General Staff. (2016) *ZDP-1(A) The Doctrine of the CAF*. Croatian MoD – CAF GS, Zagreb.

Ministarstvo obrane RH (2003) *Regulations on protection and security zones of military facilities,* Croatian MoD, Zagreb.

Ministarstvo obrane RH (2014) *Regulations on the method of securing military locations and buildings particularly important for defence,* Croatian MoD, Zagreb.

Ministry of Defence USA (1995) USA MIL-STD-810E *Military Standard: Environmental Test Methods and Engineering Guidelines,* Revision E Change Notice 3, MoD USA.

Morrison et all. (2016) *Black Core Network System and Method*, Patent No. US 9.401,920 B2.

NATO (1986) *ACE 6516/SHCPE/86 – Standard Shelter Technical Specifications*. Allied Command Europe.

NATO (2008) *C3 Interoperability Handbook for Expeditionary Operations* (NC3 IO-HB/EO), EAPC (AC/322-SC/1-WG/3)N(2008).

NATO (2014) *MC 0593 – Minimum Level of Command and Control (C2) Service Capabilities in Support of Combined Joint NATO Led Operations*, International Military Staff, IMSWM-0052-2014.

NATO (1994) *MC 337 The Military Operational Requirements and Communications Architecture for Interoperable Tactical Communications System in Support of Land Combat Forces (MOR POST 2000 TACOMS).*

NATO (2005) *NATO Network Enabled Capability, Feasibility Study, Executive Summary,* NEC FS-ES, NATO C3 Agency.

NATO (2013) *Static Networks Interconnection Policy*, NC3 Board.

NATO (2010) *TACOMS Interoperability – Augmentation of Force HQ and Tactical Capability in ISAF* (TACOMS in ISAF) – White Paper, NC3 Board.

NATO (2010) *Technical Communications in Urban Operations*, The Research and Technology Organisation (RTO) of NATO, RTO-TR-IST-067.

NATO (2009) *The Future of TACOMS*, Paper from TACOMS Blue Team, NATO C3 Board.

NATO (2002) *CIS Strategic Functional Planning Guide for Crisis Response Operations*, Supreme Headquaters Allied Powers Europe, SOCJ6/121/02, Belgium.

NATO (2008) *Directive for the Interconnection and Communications Inteoperability of Land Tactical Forces*, NC3 Board.

NATO (2017) *STANAG 2525 (AJP-6) – Allied Joint Doctrine for Communication and Information Systems*, edition A version 1, NATO Military Agency for Standardization.

NATO (2010) *STANAG 4637 – Tactical Communications (TACOMS) Phase 1 – Head STANAG*, edition 1, NATO Military Agency for Standardization.

Poularakis, K., Iosifidis G., & Tassiulas L. (2018) SDN-enabled Tactical Ad Hoc Networks: Extending Programmable Control to the Edge. *IEEE Communications Magazine*. 56 (7), 132-138. doi: 10.1109/MCOM.2018.1700387.

Ryan, M. J. & Frater, M. R. (2002) *Tactical Communications for the Digitized Battlefield*, Boston, Artech House.

U.S. Army (2019) *ATP 6-02.71 Techniques for Department of Defense Information Network Operations*. Department of the Army, Washington D.C., USA.

U.S. Army (2007) *FMI 6-02.45 Signal Support to Theater Operations* (Theater Network Support and the LandWarNet). Department of the Army, Washington D.C., USA.

U.S. Marine Corps (1998) *Communications and Information Systems*. MCWP 6-22. Department of the Navy, Headquarters U.S. Marine Corps.

About the author

Lieutenant Colonel TOMISLAV KRAVAICA (tkravaica@gmail.com) has been serving in the Armed Forces of the Republic of Croatia since 1991 – in the signal branch command and staff positions. In addition to academic civilian training in the field of electrical engineering and transport, he completed the Basic and Advanced Officer Training of the Signal Corps, and the Integral Command and Staff School. During his ten-year work at the General Staff, he participated in a series of modernization and equipping projects of the Armed Forces in the field of military-defence communication systems. Since 2015, he has been a teacher of communications at Dr. Franjo Tuđman Croatian Defence Academy where he is also responsible for development and modernization of the teaching processes.

Unaprjeđenje cjelovitosti vojno-obrambenih komunikacijskih sustava s pomoću mrežnih pristupnih točaka s naglaskom na zemaljskim radiorelejnim vezama

Sažetak

Očigledne promjene na vrlo širokom području informacijsko-komunikacijskih tehnologija ključni su pokretač ubrzanog razvoja svake sfere ljudskog djelovanja – uključujući i privatni život. U vojnoj organizaciji ovaj tehnološki napredak prisutan je kroz tzv. post 2000 koncept umrežene provedbe operacija – koji se u različitim stupnjevima implementira u vojskama širom svijeta. Nova sučeljavanja na suvremenoj bojišnici uključuju zahtjeve za sve većim volumenom elektroničkih prometnica, usložnjavanja sustava koji generiraju, dijele i konzumiraju informacijske sadržaje te prije svega što bržu dostupnost relevantnih informacija. Utrku za informacijskom superiornošću s druge strane prate nikad destruktivnije visokosofisticirane prijetnje – od klasičnih degradacija i fizičkih uništenja, djelovanja hibridnih (obavještajno-borbenih) platformi besposadnih sustava, do kiberelektromagnetskih aktivnosti napadajno-obrambene prirode. Nove paradigme višedomenskog ratovanja i očekujući scenariji koje takvi oblici angažmana donose, od suvremene vojne organizacije traže daljnja normativna uređenja unutar funkcionalnog područja vezanog uz komunikacijsko-informacijske sustave. Ona na operativno-strategijskoj razini podrazumijevaju uvođenje adekvatnih organizacijskih koncepata i doktrina, dok u provedbenom dijelu traže korigiranje ustaljenih taktika, tehnika i procedura. U takvom operativnom okružju, poseban izazov donose integrativni napori unutar vojno-obrambenih komunikacijskih sustava današnjice, pretočeni u jedinstvena cjelovita rješenja. Ključnu umreženost misijskih sastavnica osiguravaju mrežne pristupne točke. Zbog tog su razloga predmetom od posebne pozornosti mrežnih dizajnera, i u konceptualnom i u izvedbenom smislu. Učinkovitost njihova funkcioniranja, ujedno je i ocjena zrelosti vojnog promišljanja, inventivnosti i inženjerske prakse – koja će u budućim izazovima svakom borbenom sustavu donositi poraze ili pobjede.

Ključne riječi

taktički komunikacijski sustav kopnenih borbenih snaga, vojno-obrambena mreža strateške razine, cjelovitost vojno-obrambenih mreža, mrežna pristupna točka, razmjestivi komunikacijsko-informacijski sustav, MANET mreža, zemaljska radiorelejna veza, višedomensko ratovanje