DOI: https://doi.org/10.52651/sam.a.2024.1.5-14

USE OF INFORMATION TECHNOLOGY BY THE ARMY OF THE CZECH REPUBLIC FOR COMMAND AND CONTROL IN OPERATIONS

Petr HRŮZA, Ivo DUMIŠINEC, Jiří ČERNÝ, Petr GALLUS

Abstract: The aim of the article is to apply content analysis to specify the capabilities of combat sets and their abilities when employed in operations. The purpose of the article is focus on the capabilities of the C4ISTAR combat sets implemented in the Army of the Czech Republic (ACR) units. Next purpose is to examine the application of these technologies in an attempt to increase the efficiency of commanders in the implementation of command and control. Main result of the article is to describe current situation of ACR in the area of modern information technologies (IT) to support the planning and decision-making process at the tactical level. In the context of modernization, we must not forget about security - specifically cyber security. In the military environment, this is a very topical topic recently. Penetration testing can be used to verify well-set cyber security.

Keywords: Command and control; Information support; Information technology; Modular combat sets; C4ISTAR; Tactical radio communications; Cyber security.

1 INTRODUCTION

The current form and asymmetry of modern battlefields place high demands on factors that determine the nature of operations. Key factors include the availability of data and information that not only provide an up-to-date overview of the situation in the area of the operation, but are also conducive to make individual command decisions and to manage forces and assets in operations. No military expert today doubts the fact that the successful conduct of an operation means handling information effectively and purposefully. The ability to obtain, accept, process, and appraise obtained data and information as quickly as possible, and then to further distribute it along the horizontal and vertical levels of forces in an operation, is one of the most significant activities of commanders and military staff, having a substantial effect on the achievement of the objectives and the final status of a military operation. The ACR, as a fully-fledged Member State of the North Atlantic Treaty Organization (NATO), is constantly working to develop its capabilities in the field of information management. In the context of the contents of this article, this primarily concerns the implementation of C4ISTAR capability (Command, Control, Communications, Computers, Intelligence, Surveillance, Target Acquisition, Reconnaissance) in combat units and their interconnection with other types of troop units. In addition to having the necessary technical equipment (hardware), the basis for achieving this capability is software and of course the high-quality training of operators [1].

The purpose of using IT in military operations is to strive for a constant overview of the situation (situation awareness) to make the functioning of military processes more efficient. The effort to implement information management (IM) into the equipment of combat units of ACR is the attempt to accelerate the transfer of data and information. Information support enables the unit commander not only to make decisions and manage combat, but also to share these particulars, information, and decisions with other command and control bodies. The ACR actively implements combat sets into the structures of units in order to connect combat units with support units, command posts (CP), and ISR elements in the C4ISTAR system at the national and alliance level.

2 ANALYSIS OF THE PROBLEM

2.1 Application of Information Systems within the ACR

The current dynamic and rapid development of communication and information systems and technologies is enabled by the integration of new applications and programs into the environment of systems that further improve the decision-making process of the elements involved. By means of exponentially increasing computing power, these systems offer response and support in near real time to users and, according to interoperability rules, also possibilities for deployment in cooperation with alliance partners.

Information systems (IS) of command and control have been under constant development in the ACR over the last 30 years. Their development is motivated by the effort to support the information, management, and decision-making processes of the command bodies and to enable them to transform the decision of the commander (command) and their intention (operation control) towards subordinate soldiers. The crucial task is to create a common operational picture of the situation or a comprehensive overview of the deployment of units, and to display the development of the situation in the area of operation [2].

For IS, it is essential that the communication security, which is provided by means of mobile communication infrastructure, functions well. Communication systems (CS) and assets ensure the exchange of information between the sender and the recipient. Modern communication and information systems provide faster and better data transmission and processing. They serve, inter alia, to create a constant operational picture, to provide data and information in real time, and at the same time as a data database. The use of these systems reduces time and provides command authorities with the necessary information in real time. When used effectively, these systems make it possible to gain information superiority over the enemy [3,4].

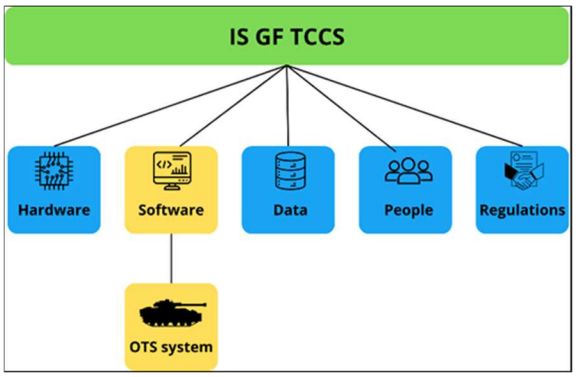

Fig. 1 IS GF TCCS Architecture
Source: [own].

In its Ground Forces, an „Ground Forces Tactical Command and Control Information System" (IS GF TCCS) has been introduced and used by the ACR to work with information and data.

It is a complex computer program with integrated application software (ASW); this system is divided into two components:

- the combat vehicle information system (BVIS) SAMET, which is intended for the transfer of unclassified information among battalion units and the battalion CP. This system is installed at the battalion in the assets of the wheeled combat vehicle Pandur II (WCVP), VRp, R5M1p, R6M1p, R7M1p and, after the acquisition and modernization of radio stations, a newly implemented wheeled armored vehicle command - staff (WACS),
- the operational tactical system is the system (OTS) DOLPHIN, which is designed to transfer information to the classified level „confidential" within the place of command (PC) of the battalion, brigade and superior levels. This system is installed at the battalion within the workplaces of the main command center [5].

The environment of these systems implicitly offers individual items (applications, editors) and at the same time allows you to choose and switch among individual ASW functions. The systems make it possible to create documents using editors or predefined forms, or to create them in an office package, to provide them with the appropriate level of classification, and to distribute them to the authorized users. Command authorities can create a variety of documents, formalized reports, reports, plans, and combat orders with minimal effort using created and predefined documents. The environment also makes it possible to notify and warn subordinate forces and assets (signals) [2].

The MIP Protocol (Multilateral Interoperability Programme) also enables not only the creation and distribution of documents, but also the exchange of data and information during joint operations in a multinational environment. Other editors used for command and control units are the task editor, the event editor, the status editor for one's own resources, and enemy event records. The editor for plans and orders allows users to completely create within a defined structure OPORD (Operation Order), FRAGO (Fragmentary Order), and WARNO (Warning Order) [3].

Other (supporting) applications can be used to support the decision-making process of commanders. These include, for example, the service of the operational tactical application, which is suitable for planning the deployment of reconnaissance elements (optical visibility), connecting retransmission nodes (radio visibility, RRL), and planning the movement of units (or enemy) within the operation (relief visualization). Additionally, it is possible to use applications displaying operating times, applications allowing users to calculate the sum of combat values of deployed elements (force ratio) when selecting variants, to determine the speed of vehicle flow (movement on roads), to perform an analysis of the quality and the connection strength (analyzing the RRL connection), and to compute other elements within the command of the operation, etc. [4,6]

The concisely analyzed systems used in the ACR are dependent on ensuring sufficient transmission speeds and the timely transfer of important information to the right place. In contrast to the irrefutable advantages, the disadvantages of these systems must also be mentioned, especially in the area of measures to protect information during its transmission. This mainly concerns the classified transmission of data, restricting access of the unauthorized persons to sensitive information, and cryptographic protection. All these measures must be constantly improved, updated, and constantly developed. It is also necessary to take into account the environment of the operation and the possibilities of one's adversaries, especially in areas where systems are susceptible to the interruption of information flow from individual sensors (for instance, a disintegration of information flow occurs when disabling a transit node), in the event

of an attack with a nuclear electromagnetic pulse by the adversary, all electronic components operating on the basis of transistors that are in operation at the time of the explosion may be disabled. And the last example of a negative impact is electromagnetic interference by the adversary, performed by electronic combat (EC) units, which affects the data flow by disrupting it, altering it or influencing it with misleading information.

2.2 C4ISTAR Architecture

The basic multiplier of the forces of advanced armies is C4ISTAR architecture. Its main purpose is to ensure adequate situational awareness of all soldiers, and to enable the most effective command and control at all levels of command and control (C2). With its assistance it is possible to obtain data and information, especially seeing at night, conducting fire support, and carrying out reconnaissance without the need for any physical presence in the area. C4ISTAR architecture makes a vital contribution to the protection of forces and the precise deployment of weapons and ammunition. Therefore, it saves human lives and reduces the logistical complexity of units. Its principle lies in the effective use of the electromagnetic spectrum for command, control, communication, data processing, military intelligence, surveillance, target acquisition and reconnaissance. It enables the digital connection of sensors with assets for data processing, transmission, and analysis. The outcome is a system applicable across the organizational levels of troops. At the level of small units, it supports the decentralization of command and control as well as autonomy of action on the battlefield. From the perspective of current operations, C4ISTAR architecture is a key element for the asymmetric (non-linear) battlefield. Its individual parts provide [7]:

- command in a unified digitized map environment;
- control on the basis of compatible navigation, location – position and acquisition data;
- communication via standardized waveforms and protocols;
- data processing in a way that corresponds to the organizational level and needs of the unit;
- military intelligence across organizational levels with a unified datalink;
- surveillance according to the needs and reach of the unit, during both daytime and nighttime;
- acquisition of a target for military intelligence and fire support;
- reconnaissance with the possibility of direct and indirect action in the area of interest.

Appropriate components are available for each of these functionalities at individual organizational levels. Vertical integration of these components allows the appropriate use of interoperable technologies in a way that meets the requirements and logistical capabilities of individual units. The horizontal integration of these components supports the creation of complete sets for deployment at individual organizational levels [8].

2.3 Modular Combat Sets

In order to create s unified C4ISTAR environment (for the technological and operational interconnection of combat units at the platoon and company levels), the acquisition process (purchase and armament) of combat units was commenced in the ACR at the beginning of 2016. For the Rapid Deployment Brigade, modular combat sets (MCS) were gradually introduced into combat units (airborne, mechanized). The aim of this process was to systematically connect combat units with combat support units, CP, and the ISR units in the C4ISTAR system at the national and alliance level through the implementation of MCS. The aim of the project is to ensure the capabilities of combat units in obtaining and maintaining an up-to-date overview of a common picture of the situation [8].

MCS represent a multi-level combined system of command, control, communication, datalink, intelligence, surveillance, reconnaissance, and target setting to extend the existing command and control system. The purpose is primarily the collection and immediate appraisal of information in the operational area, but it also mediates the transfer of data from units of unmanned aerial assets, fire support of artillery, and the air force. The MCS ISTAR architecture is based on the effective and systematic application of the electromagnetic spectrum in order to achieve sensory and information dominance in the area of conducting combat operations.

2.4 Modular Combat Sets Technical Support

The Czech soldier system bears the designation SSR TA (Sensor Surveillance Reconnaissance, Target Acquisition) within the MCS and takes the form of three sets:

- a small set for a team (SS SSR TA (T));
- a small set for a platoon (SS SSR TA);
- a large set for a company (LS SSR TA) [9].

The common factor of all three versions is the MANET network (MOBITE AD HOC NETWORK) with the high-speed waveform WaveRelay and MIMO option (MULTIP1E-INPUT, MULTIPLE-OUTPUT), enabling the transmission of information at speeds up to 150 Mbps [9].

The Czech SSR TA system is operated in the frequency range 1,350 MHz to 1,390 MHz, i.e. in the band used within NATO for the most modern communication networks of small units. ACR units most often use a 5 MHz channel, systemically set up for thirty participants (the equivalent of a combat platoon). Communication security (COMSEC)

is based on the application of the AES (Advanced Encryption Standard) key and complies with the requirements of Suite B of the US National Security Agency (NSA). Management of information transfer is provided by the situational firmware MyVector, built on the web server of the same name with a Linux operating system, enabling the mutual integration and connection of other components [9].

The system also includes the MyTS sensor interface (tactical sensors), the MyUI system interface (user interface), and the MyVector OL web client (open layers) for working with map data. The MySQL (structured query language) database system is used to store and manage the obtained information [9].

The sensor interface allows various types of ISTAR architecture components to be connected to the data terminal. For instance, optoelectronic elements such as digital cameras and laser rangefinders, or terminals of the ROVER type (Remotely Operated Video Enhanced Receiver), tactical radio stations and control stations of UAVs (Unmanned Aerial Vehicle), UGVs (Unmanned Ground Vehicle) and UGSs (Unmanned Ground System) such as sensors and radars.

The basis of the system interface is one of three digitized map materials (raster, vector, and orthophotomap), which can be enlarged or reduced while displaying the current scale. Furthermore, it is possible to use tools for drawing in a digitized map, including the measurement of lengths and areas or the conversion of obtained data among individual coordinate systems. Thus, it is possible to mark on the map dangerous areas, places of concentration, points of interest, etc. These tools also include a message-writing function (similar to SMS) and photo production (similar to MMS). All these objects can be further shared with other network participants equipped with data terminals [5, 9].

An analog image from optoelectronic sighting devices, observation devices, or output captured by digital cameras, camcorders and smartphones, can therefore be converted and distributed to the network. Personal, manual, portable and transportable acquisition units represent one of the greatest sensory benefits of the system, and enable not only surveillance of the target, but also measurement of its distance, direction, or even coordinate position. They are used not only for surveillance and reconnaissance, but also play a very important role in the acquisition of targets, in the use of combat support units (snipers, ATGM, mortars), and fire support for artillery and air force.

2.5 Modular Combat Sets Combat Support

Lethality and mobility are one of the most important characteristics of ground combat units. Within the form of current conflicts there is a growing need to deploy ground units in the form of separate infantry elements that depend on infantry redeployments and a high level of autonomous security. Thus, the ability to navigate and coordinate these dismounted elements on the battlefield, and to ensure cooperation with elements of combat support, such as fire support, comes to the fore.

The SSR TA system is based on audiovisual communication that is easier to understand and clearly displayed. For this reason, the SSR TA network cannot be understood as a replacement, but rather as a parallel system to the existing C2 command and control networks. The SSR TA system must therefore be seen as a tactical intranet, fully independent from fixed infrastructure. Its main goal is to obtain information and data to support the situational awareness of commanders and to promote sensory dominance over the adversary.

The basic tool of the SSR TA system, common to all versions, is the tactical hub MPU (Man Portable Unit) in the form of a personal terminal. The MPU-5 terminal looks like a personal radio, but it is actually a computer with an Android operating system with a built-in GPS receiver, video decoder, detachable radio module, three flat system connectors to allow you to connect peripherals via the interfaces Ethernet, USB, and a connector for connecting an analogue video source. The main task of each MPU-5 terminal is to actively participate in the creation of the MANET network, thereby contributing to its robustness, performance, and reach [9].

Another common component of MCS which connects all the levels of MCS, is the ruggedized MyVector 5 data terminal, which is attached to a special chest strap. It enables working with map data, the user monitors the positions and movement of other members of the unit and is able to command them effectively [9].

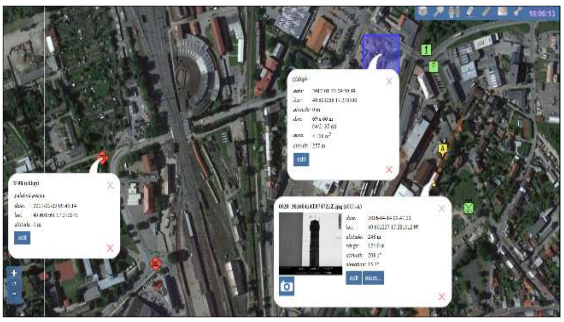

Fig. 2 Output example of the ortophoto map in MyVector 5
Source: [own].

The MyVector 5 terminal is connected to the hand-held radio AN/PRC-148C IMBITR (Improved Multiband Inter/Intra Team Radio) with the FMV-MM module (full-motion video mission module). The FMV-MM module, powered and controlled from the IMBITR radio, belongs

to the ROVER group of terminals. This functionality allows you to share video outputs from unmanned aerial vehicles (all available types such as Wasp, Raven, Scan Eagle ad Predator) for all the members equipped with MCS [9,10].

Other very modern and efficient elements of MCS are the acquisition units MOSKITO IT and JIM COMPACT. The hand-held acquisition unit MOSKITO IT, with a weight of just 1.2 kg and the possibility to control it with only one hand, is the main sensory system of the platoon SS SSR TA, offering a daytime channel and an uncooled thermal imaging channel. It is also possible to use an optoelectronic channel, a laser rangefinder, a digital compass and inclinometer, and a GPS receiver. The MOSKITO IT allows users to monitor the area of combat activities beyond the effective range of hand-carried weapons (2,500 meters) during daytime and nighttime. This ensures the search for targets and possible threats well in advance and thus effectively supports the selected firing system of the unit on the battlefield. All captured videos and photos can of course be shared on the MANET network for the needs of other users. The technology for sharing the scanned image online or IN TIME through the MyVector 5 terminal is very advanced [11,12].

The 2 kg JIM COMPACT unit is a company-based surveillance platform that includes a cooled thermal imaging camera, a high-resolution color daytime camera, as well as a MOSKITO IT laser rangefinder, digital compass and inclinometer, and a GPS receiver. It does not possess a daytime surveillance branch, but it can still detect the movement of people at a distance of 6 km and combat equipment up to 10 km, regardless of the time of day. The maximum operating time of the battery is 4 hours [11,12].

As is apparent from the foregoing, SSR TA sets should not be a burden, but assets enabling small units to multiply their capabilities, not only in classic linear, but especially in increasingly frequent and confusing asymmetric operations. MCS can be considered as multipliers of the capabilities of ACR combat units.

2.6 Current Restrictions and Limits

Currently, the ability of the system is set communication-wise to the level of team–platoon–company connection, which positively affects the ability and support for timely information about the adversary, and the possibility for the tactical reconnaissance of areas of interest at the lowest tactical level. Adequate technical assets for the transmission path have not been created for the correct operation of the system containing security of the required information transfer towards the intelligence group of the staff.

In the event of identifying information, the intelligence group of the battalion staff is able to analyze, process, appraise, and further distribute the received data to other interested elements of the tactical infrastructure, with added value in the form of detailed data and the creation of inputs to unit warning systems.

Adequate assets would be, as part of the process of modernization, the deployment of radios from the same manufacturer HARRIS, using the same type of data transmission (ANW2C) in the facilities at the command post of the battalion. At present, the facilities of the radio network for the command and control of reconnaissance (network containing embedded reconnaissance bodies and elements) are operated on the equipment of the wheeled combat vehicle Pandur II (WCV-Pz, WCVP-PzLok) and R7M1p, where the RF and R-150MX series radios have been implemented; these radios do not have data compatibility with the technical assets of the MCS system.

3 DISCUSSION

3.1 Functionality of the System by Means of Complex Organization and Architecture

Finding a solution to the above-mentioned shortcomings is the ultimate goal, thereby achieving a functional and fully interconnected system of tactical radio communication (STRC). And this with the help of modern MCS technologies and the unification of C4ISTAR technologies with the effective integration of new communication systems to meet the current requirements for a modern command and control system.

The ACR tactical radio communications system provides a continuous secure radio connection in order to deliver C4ISTAR capabilities from the individual to the brigade task force commander. To this end, we need to define several fundamental requirements of the contemporary battlefield for the ability of communication and information support of deployed units:

1. The STRC architecture must be open, but managed across the operating environment, without additional technological and security constraints. It must allow the integration of new elements of the battlefield without the need for major intervention in existing systems.
2. The architecture must support an agile approach, not only in the deployment of units, effectors, weapon systems, sensors, but also for alterations in the configuration and organization of connections forced by the situation on the battlefield.
3. One of the fundamental requirements of the contemporary battlefield is to ensure information and cyber security, and a unified approach to cryptographic protection at all the levels of C2.

4. The architecture must be designed so robustly that it is prepared to withstand the explosion of data coming from current assets of the battlefield so that there is no overload of individual parts of the infrastructure during their transmission and processing.
5. Deployed assets of communication and information support must create the conditions for increasing the resilience of the entire STRC to the effects of the adversary's electronic warfare assets.
6. Given the dynamics of the contemporary battlefield, it is essential that a solution is used to integrate the basic functions of C4ISTAR that supports interoperability, mutual cooperation, and acceleration of the decision-making process.
7. In order to secure the connection system within the STRC ACR architecture, it is necessary to achieve comprehensive organization in the connection of units in the form of P. A. C. E. (primary, alternative, contingency, emergency).

Listed requirements were developed and made on the basis of conducting expert interviews. Expert interviews were conducted at the tactical level with members of battalions/brigades CP and users of MCS technologies. At the operational level, the proposals were formulated after discussion with members of the ACR Communications and Information Services Agency, which is the entity responsible for the development of IT technologies and complex management of the overall command and control architecture of the ACR.

Based on the above-mentioned requirements, the architecture must be divided into the following basic building blocks, i.e. datalinks (channels):

- Tactical datalink (national);
- Sensory datalink (alliance and national);
- Technological datalink (national).

3.2 Tactical datalink

The tactical datalink is primarily intended for the secure voice and data communication of individuals, teams, platoons, companies, combat platforms with a superior level, or command posts, and among units within the tactical communication C2 or C4ISTAR ACR. The tactical datalink is realized by multi-band radio stations, in vehicle, portable, hand-held or personal configurations.

To get the required capabilities of the tactical datalink, it is necessary to choose multi-band radios with a TYPE-1 fully-fledged encryption algorithm, which is compatible within NATO. These radios are obligatory in terms of building architecture, especially in terms of the compatibility of waveforms, including connection to vehicle intercoms and other integration platforms. In terms of the use of the tactical datalink in the air force for the capability of air-to-ground communication, aircraft radios must be fully compatible in the operating modes and at least in the waveforms VULOS, HAVEQUICK I/II, SINCGARS and ANW2C [14].

At present, the radios of several manufacturers are used in the ACR, some of which do not allow for full integration into the tactical datalink. Their current configuration only allows integration based on unclassified voice transmission, or they operate on a fixed frequency basis and are not capable of full integration into a managed and open, federated architecture.

L3HARRIS radios in the AN/PRC model series are technologically suitable for creating the above-mentioned tactical datalink. Like for instance the AN/PRC-150 FALCON II, AN/PRC-152 FALCON III, AN/PRC-160 FALCON IV, AN/PRC-163 FALCON IV and AN/PRC-117G. Or personal radios RF-9820S, RF-7850S PR, RF-330M DL (SSDL) and RF-335A DL (SSDL), and the hand-held or vehicle terminal BGAN of the RF-7800B radio [10].

3.3 Sensory datalink

The sensory datalink is especially used to ensure the data communication of sensor elements applied in units for the transmission of sensory data (video, metadata, audio). Thus, in the context of sensory datalink, the data is transferred between the sensor and the sensor control element or the receiver outputs from the sensor. A typical example of a sensory datalink is the transmission of metadata (video, data, position) from an unmanned aerial vehicle or an unmanned ground vehicle. In the case of electronic warfare, such as interference of the sensory datalink, the C2 and C4ISTAR systems are not affected in any way.

It is necessary to divide the sensory datalink into a) alliance (NATO), which is represented by ROVER type receivers and complies with STANAG 7085, and b) national, which is represented by the WaveRelay waveform and is for securing sensory data within the ACR [13].

To get the required capabilities of the sensory datalink, it is essential to choose radios and receivers with the AES-256 encryption algorithm, a unique frequency for vehicle platforms, and the possibility to have the same bandwidth for all the units. Assets providing adequate capabilities for sensory datalink are, for instance, Rover 6i and TNR (Tactical Network Rover) receivers, or GVR-5 and MPU-5 devices [10].

3.4 Technological datalink

The technological datalink is used to ensure solely data communication of the vehicle and technological units of combat and reconnaissance platforms. The technological datalink is therefore used mainly for transmitting technical and configuration data.

In the context of technological datalink, data is therefore transferred between the combat platform and the control element, or the service or configuration element. A typical example of the technological datalink is the transmission of control and configuration data (control, position) from an unmanned aerial vehicle (miniVTOL) or an unmanned ground vehicle (UGV). At the same time, this datalink can be used to retransmit the MANET technological network in the required band. In the event of interference with the technological datalink, the C2 and C4ISTAR systems are not affected in any way.

From the perspective of the activity of the architecture, this datalink plays an irreplaceable role in the diagnostics of combat platforms in relation to service and maintenance activities. The basic advantage of the technological datalink is the ability to transfer large volumes of data from one configuration location, or the application of uniform settings for all combat platforms without the need to build a remote network infrastructure [14].

As part of increasing the ability of diagnostics and service activities, this datalink can be used to fulfill the ability of the "Technological BFT". The designation BFT (Blue Force Tracker) allows support units to search for combat platforms on a map base, without the need to enter the channel C2 with situation awareness support [14].

In order to get the required capabilities of the technological datalink, it is necessary to choose assets that enable the overall compatibility of waveforms, including the connection to integration platforms. Assets that provide corresponding capabilities for the technological datalink are, for instance, the GVR-5 and MPU-5 [10].

3.5 Cyber security

The previous text dealt with connections and means of connection. A secure connection was also mentioned. The development of communication and information systems brings, in addition to unquestionable benefits, also new threats and risks. Recently, there is a need to address security as a whole, especially with a focus on cyber security.

Cyber security deals with the security of all information throughout its existence and is closely related to cyberspace. Future wars will not take place on the battlefield, but mainly in cyberspace.

The 2016 NATO Summit in Warsaw recognized cyberspace as the fifth operational domain. Cyberspace is the fifth domain of war, and therefore this issue needs to be addressed. The technical/ technological security of all systems has been addressed for several years and is at a very good level. It is just necessary to follow the rules. The biggest threat to cyber security is an insufficiently trained or insufficiently knowing soldier. Penetration into any military information or communication system is not so simple. The main goal of the enemy will be to obtain valuable data about the arms industry. Another goal may be to infiltrate an information system or an opponent's server and replace its contents with data created by an attacker. Information operations conducted in cyberspace also gain in importance, with the aim of influencing the thinking and possibilities of the enemy. It is the use of cyber capabilities and capabilities of individual armies or states to achieve goals in cyberspace that can be understood as a cyber operation. Cyber attacks make it possible to strike and endanger the functioning of public administration, critical infrastructure (such as electricity or water supply), the financial sector, they can endanger the security of important objects, and they are means of espionage and disinformation campaigns. Therefore, the issue of cyber security must be addressed not only by individual states, but also by armies and also by the soldiers themselves. It is a person or a soldier in case of military environment that is the weakest link in the whole system.

3.6 Penetration testing of military IT systems

Penetration testing of military Information Technology (IT) systems plays a crucial role in maintaining national security and operational readiness. Given the increasing sophistication of cyber threats, regular and comprehensive penetration tests are indispensable for identifying vulnerabilities and ensuring the resilience of these critical systems.

Unlike conventional IT environments, military networks host highly sensitive data and control mission-critical operations, making them prime targets for adversaries. The objective of penetration testing in this context is not only to detect exploitable weaknesses but also to assess the potential impact of such vulnerabilities on national security and military operations. By simulating real-world cyber attacks under controlled conditions, military organizations can evaluate their defensive mechanisms, improve incident response strategies, and enhance the overall security posture of their IT infrastructure. This proactive approach is vital for preventing data breaches, maintaining the integrity of military operations, and safeguarding national interests against the backdrop of an evolving cyber threat landscape.

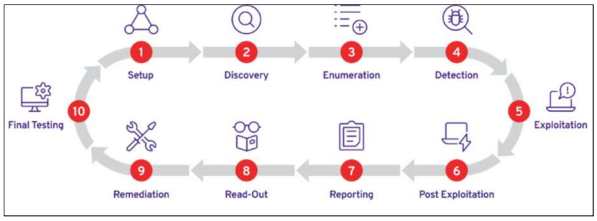

Fig. 3 Penetration testing process in steps
Source: [19].

Historically, military intelligence was the gestor, responsible subject and executor of penetration tests of IT systems of the Czech Armed Forces. In 2024, this role will be partially transferred to the Cyber Regiment, or its newly established department, which will be dedicated to penetration testing not only of field IT systems used in operations. This department is currently being set up administratively and in terms of personnel, the technical and legal boundaries of penetration testing processes are being defined and its operation is planned for the second half of this year.

3.7 General comparison

Comparing the IT used by the forces and assets of the ACR at the CP with other armies of NATO member states is always problematic in similar studies (articles), as they are usually subject to the "SECRET" level of secrecy. However, for ACR units operating in foreign operations (in NATO and EU BG operations), the ACR Communications and Information Services Agency ensures connection with stationary communication and information systems via the Automated Command and Control System (ACMS). The operation of information systems to support the department's administrative activities, such as operational-tactical system (OTS), SIS (staff information system), internet of the Ministry of Defense (IMO) and also functional services such as FIS (financial information system), ISL (information system of logistics), ISSP (integrated service and personnel subsystem) and others. In this way, the management of units from the level of the permanent operations centre (SOC), logistics and personnel support is also ensured. All alliance units have a similar IT structure and related systems. To date, the ACR has not deployed and approved a security mechanism enabling the seamless exchange of data between alliance and national stationary command and control systems (Static Network). A security mechanism enabling the seamless exchange of data between the stationary (Static Network) and deployable (Deployable Network) information systems of ACR is not deployed and approved due to their different degree of secrecy. Interoperability of CIS units of land and air forces at the national level is not fully ensured.

4 CONCLUSION

From the foregoing it follows that the architecture of tactical radio communications provides for the comprehensive treatment of radio communications on a modern battlefield in the context of national and international relations. It is therefore necessary for this concept of architecture to be adopted by all types of units on the battlefield, not only by ground units, but also by airborne and special units. In addition, in the context of ground forces, the acquisition process of the modernization of the ACR must be uniform for all types of troops. This is the only way to achieve comprehensive compatibility among the different troop types.

For the future successful development and implementation of new technology in the ACR, it is crucial to ensure the harmonization of all previously developed concepts for the development of the ACR in individual functional areas. The newly prepared concept of ACR command posts can be given as an example. This will result in the functional interconnection of all elements and increase the effectiveness of conducting combat operations within a modern battlefield, a successful confrontation with the tools of hybrid conflicts and information operations, as well as the reduction of secondary impacts on the civilian population [15].

Effective deployment of military forces in diverse operations requires the widest possible support of modern information technologies. Mathematical algorithmic models, using a raster representation of geographic and tactical data described in [16,17], represent one of them. Utilization of such software will provide commanders with substantive independence and speed of decision-making in the course of military operations [18,19]. Sharing designed maneuver routes or observation posts with all adjacent units and higher headquarters also enables to coordinate the activity of all superior task forces.

References

[1] Jednotné prostředí C4ISTAR [online]. [cit. 2021-05-25]. Available at: http://www.infrared.cz/domains/infrared.cz/projekty/istar.html

[2] STODOLA, P. *Informační podpora rozhodovacího procesu velitele.* Praha: PowerPrint, 2018. 160 s. ISBN 978-80-7568-105-8.

[3] ČERNÝ, J. *Vojenský plánovací a rozhodovací proces v operacích.* Praha: Powerprint, 2019. ISBN 978-80-7568-160-7.

[4] ČERNÝ, J. a DUMIŠINEC, I. *Úvod do studia předmětu Taktika a velení v operacích: study text.* 2020. ISBN 978-80-7231-412-6.

[5] Systémy C4ISTAR pozemních sil [online]. [cit. 2021-5-25]. Available at: https://www.iczgroup.com/produkty-a-sluzby/obrana/systemy-c4istar-pozemnich-sil/

[6] The Battle Staff. *Leading, Planning and Conducting Military Operations.*

SMARTBook. The Lightning Press. Fifth Edition. ISBN 978-1-935886-63-1.

[7] ATP-77. NATO guidance for ISTAR in land operations. Brusel (Belgium): NATO standardization agency, 2013.

[8] ŠNAJDÁREK, P. *Projekt Modulárního bojového kompletu (MBK) pro podporu C4 ISTAR AČR* (presentation). Praha: 2016.

[9] CHLUP, V. *Jemná mechanika a optika.* Roč. 61, č. 9, 2016. Praha: Fyzikální ústav Akademie věd České republiky, v.v.i. ISSN 0447-6441.

[10] L3Harri s Public Safety and Professional Communications Products & Services Catalog [online]. 2020. [cit. 2021-05-25]. Available at: https://www.l3harris.com/sites/default/files/2020-12/cs-pspc-products-services-catalog-nov-2020.pdf

[11] Portable Optronics for infantry: Handheld and multifunction binoculars for infantry [online]. France: Safran Electronics & Defense, 2016. [cit. 2021-5-25]. Available at: https://www.safran-group.com/companies/safran-electronics-defense

[12] Produktový list: vectronix moskito. Vectronix AG [online]. [cit. 2021-05-25]. Available at: http://www.vectronix.ch/userupload/557_MOSKITO_brochure.pdf

[13] FIALKA, V. a KNAPEK, V. Odborné shromáždění Ředitele Sekce KIS Ministerstva Obrany ČR: *Koncepce taktické radiové komunikace (lecture).* Olomouc, 18. - 19. 5. 2021.

[14] FIALKA, V. a KNAPEK, V. Odborné shromáždění Ředitele Sekce KIS Ministerstva Obrany ČR: *Systém taktického spojení Pozemních sil AČR jednotlivec, družstvo, četa, rota (presentation).* Olomouc, 18.-19. 5. 2021.

[15] NOHEL, J. 2019. Possibilities of Raster Mathematical Algorithmic Models Utilization as an Information Support of Military Decision Making Process. In Mazal, J. (eds) *Modelling and Simulation for Autonomous Systems.* MESAS 2018. Lecture Notes in Computer Science, vol. 11472. Springer, Cham. Available at: https://doi.org/10.1007/978-3-030-14984-0_41

[16] STODOLA, P., DROZD, J., NOHEL, J. and MICHENKA, K. 2020. Model of Observation Posts Deployment in Tactical Decision Support System. In Mazal, J., Fagiolini, A., Vasik P. (eds) *Modelling and Simulation for Autonomous Systems.* MESAS 2019. Lecture Notes in Computer Science, vol. 11995. Springer, Cham. Available at: https://doi.org/10.1007/978-3-030-43890-6_18

[17] NOHEL, J. and FLASAR, Z. 2020. Maneuver Control System CZ. In Mazal, J., Fagiolini, A., Vasik P. (eds) *Modelling and Simulation for Autonomous Systems.* MESAS 2019. Lecture Notes in Computer Science, vol. 11995. Springer, Cham. Available at: https://doi.org/10.1007/978-3-030-43890-6_31

[18] NOHEL, J., STODOLA, P. and FLASAR, Z. 2021. Combat UGV Support of Company Task Force Operations. In Mazal, J., Fagiolini, A., Vasik, P., Turi, M. (eds) *Modelling and Simulation for Autonomous Systems*. MESAS 2020. Lecture Notes in Computer Science, vol. 12619. Springer, Cham. Available at: https://doi.org/10.1007/978-3-030-70740-8_3

[19] ZINSZER, D. 2023. Hack the 10 steps of the pentesting routine - PlexTrac. PlexTrac. Available at: https://plextrac.com/hack-the-10-steps-of-the-pentesting-routine/

Col. Assoc. Prof. Dipl. Eng. Petr **HRŮZA**, Ph.D.
Vice-Rector for Education and Students Issues
University of Defence
Kounicova 65
662 10 Brno
Czech Republic
E-mail: petr.hruza@unob.cz

Maj. Dipl. Eng. Ivo **DUMIŠINEC**
Universtiy of Defence
Faculty of Military Leadership
Department of Tactics
Kounicova 65
662 10 Brno
Czech Republic
E-mail: ivo.dumisinec@unob.cz

Ltc. ret. Dipl. Eng. Jiří **ČERNÝ**, Ph.D.
University of Defence
Faculty of Military Leadership
Department of Tactics
Kounicova 65
662 10 Brno
Czech Republic
E-mail: jiri.cerny@unob.cz

Lt. Dipl. Eng. Petr **GALLUS**
University of Defence
Faculty of Military Technology
Department of Informatics and Cyber Operations
Kounicova 65
662 10 Brno
Czech Republic
E-mail: petr.gallus@unob.cz

Col. Assoc. Prof. Dipl. Eng. Petr HRŮZA, Ph.D. - Graduate from Computer Technology and Automated Command – Electronic Computers. He acquired the academic doctoral degree in Troops Control and Engagement field. He was conferred docent (associate professor) degree in „Military Management" field. His academic career began in 1995. His research efforts focus on cyber security and defence, critical information infrastructure, and military information and communication systems.

Maj. Dipl. Eng. Ivo DUMIŠINEC - Graduated from the University of Defence in 2009. He majored in Tactics and Military Management. He spent his professional career as a member of 4th Rapid Deployment Brigade for 10 years. He actively participated in NATO exercises in Germany, Norway and the Netherlands. His academic career has begun in 2018. His main area of expertise is in tactic, command and control issues, command post on battalion level equiped by new IT technology and procedures to ensure efective and secure C2.

LTC ret. Dipl. Eng. Jiří ČERNÝ, Ph.D. - He graduated from the Military College of the Ground Forces. He served in command and staff positions in combat units, and brigades. He participated in the international SFOR mission, worked as Chief of Staff in the multinational brigade in Slovakia and worked at the Operational-Strategic Headquarters of the European Union. In 2006, he joined the University of Defence as an academic worker at the Department of Tactics. He deals with the issue of tactics and command and control.

LT Dipl. Eng. Petr GALLUS - Cybersecurity professional and researcher working in the Czech army. After graduating in IT, he continues his PhD program focused on cybersecurity. He focuses on ethical hacking and finding vulnerabilities in IT systems, and he is the creator of the task for the finals of the national championship in cybersecurity. Author also organizes educational and professional lectures for the public.