



Internet of Things in military applications

Vlada S. Sokolović^a, Goran B. Marković^b

^a University of Defence in Belgrade, Military Academy,
Department of Logistics, Belgrade, Republic of Serbia,
e-mail: vlada.sokolovic@va.mod.gov.rs, **corresponding author**,
ORCID iD:  <https://orcid.org/0000-0003-0782-0506>

^b University of Belgrade, School of Electrical Engineering,
Belgrade, Republic of Serbia,
e-mail: gmarkovic@etf.bg.ac.rs,
ORCID iD:  <https://orcid.org/0000-0002-6638-8058>

DOI:10.5937/vojtehg71-46785; <https://doi.org/10.5937/vojtehg71-46785>

FIELD: telecommunications, information technologies

ARTICLE TYPE: review paper

Abstract:

Introduction/purpose: The term Internet of Things (IoT) usually refers to the collective network of connected devices and the technology that facilitates communication between these devices and the cloud, as well as among these devices. The IoT concept is lately considered and applied as the appropriate in design of systems intended for distribution of data and information between heterogeneous devices with the aim to improve efficiency and effectiveness of business and decision making. The IoT enables energy and supply chain monitoring, production coordination, equipment performance optimization, transportation, public health, and improves workers' safety and health. In addition to smart devices, IoT technology also enables the connection of various sensors as a source of data on various physical phenomena, and, based on the information obtained, it is possible to control the operation of devices, make predictions, make decisions, etc. In this paper, specific areas of the application of the IoT in the defense and security sector are analyzed in order to identify the possibilities of applying modern technologies in raising the defense potential of the state and define the directions of future research in the subject area.

Methods: The methods of content analysis of current research were applied, and then, with the deductive method, conclusions were reached about the future directions of the development of IoT technology.

Results: A detailed analysis of past and ongoing research in the defense and security sector was carried out, and potential directions of future research into the IoT were given in order to increase the operational capabilities of armed forces.

Conclusion: IoT services will certainly contribute to a greater degree of automation and improvement of the quality of military decisions on the

battlefield, especially in the conditions of unexpected scenarios in an unpredictable hostile environment, thus facilitating the reduction in both human and material losses in operations.

Key words: internet of things, defense and public safety, internet of things applications, localization and target detection, military logistics.

Introduction

The Internet of Things (IoT) presents an effective concept of a system for collecting and distributing data and information between heterogeneous IoT devices and application servers with the aim of efficiency and effectiveness improvement in all types of business and decision-making processes. The introduction of the Internet of Things enables huge improvements in a wide range of application areas, such as energy monitoring, supply chain monitoring, production coordination, equipment performance optimization, transportation, public health, infrastructure monitoring, and improvement of worker safety and health (Fraga-Lamas et al, 2016).

IoT based systems have a very broad field of applications and there are estimates that these connect several tens of billions of devices in machine-to-machine (M2M) communication. Also, it is widely assumed that IoT systems deployment will enable the automation of everything in the human environment. In addition to smart devices, Internet of Things technology also enables connecting various sensors as sources of data on various physical phenomena (Zhu et al, 2021). The gathered information that describes current events in the environment is then transmitted through communication networks to a computer – application server, where the gathered data is analyzed, classified and processed through various software applications. Based on the obtained information, monitoring of data distribution on the network, device operation control, forecasting, decision making, etc. are enabled.

IoT technology has been proven suitable for systems that manage a large number of disparate devices and equipment in order to facilitate more efficient coordination of complex processes. The increasing number of Internet connections, the rapid advance of sensor technology, and the increase in the flow in the distribution network has made IoT technology an interesting area for the research in the fields of defense and security (Pokorni, 2019).

The basic characteristics of IoT technology are (Vermesan & Friess, 2014):

- Interconnection: there is a possibility of connecting different devices (electronic and mechanical ones) in the global information infrastructure,
- Things-oriented services: online services are adapted to things due to physical limitations, security requirements or communication protocols,
- Heterogeneity: devices of different configurations and manufacturing technologies can communicate through different networks (using different open and proprietary protocols),
- Dynamic environment: online communication allows working with devices that change their physical location, speed of movement and with the temporary absence of connection, and
- Enormous scale: An increasing number of devices connected to the network is expected, as well as an enormous amount of data generated by these devices that need to be managed and adapted to the needs of applications - users.

In this paper, the specific areas of the application of the IoT in the defense and security sector were analyzed in order to identify the possibilities of modern technologies application in raising the defense potential of the state and define the directions of future research in the subject area.

The following Figure 1 presents the most important areas of the application of IoT technology for defense and public safety purposes.

The modern Network-Centric Warfare (NCW) paradigm aims to transform the conventional military concept through the policy shift towards expanded communications gateways, and by connecting battlefield assets with the command (headquarters) (Abdelzاهر et al, 2018a). In the NCW approach, through the sharing data between legacy assets and novel deployments, the significant advantages can be achieved through the force projection and the secure timely exchanged information among all entities. This way, the physical domain, in which data is generated regarding the event locations and operations, the information domain, in which the storage, processing and transmission of data and information is conducted, and the cognitive domain, in which all the gathered data is filtered, processed and analyzed in order to allow proper information extraction and support decision-making process, can be fully integrated in order to enable the joint operation of these domains including the ability to perform joint optimization related to specific tasks.



Figure 1 – The main application areas of IoT technology in defense and public safety sectors

Рис. 1 – Основные области применения технологий Интернета вещей в области обороны и общественной безопасности

Слика 1 – Главне области примене ИIoT технологије у сектору одбране и јавне безбедности

In fact, these three domains of the NCW paradigm can be directly translated into the basic elements of modern commercial IoT technology. As a result, the adoption of IoT-based systems in key areas of modern military and homeland security areas can be considered. This conclusion is additionally supported by the contemporary aspiration in defense sector to partially equip the units with the basic functionalities provided by the COTS (Commercial of the Shelf) solutions, such as smart phones, RFID (Radio-Frequency Identification), sensors, etc. Therefore, defense applications still present one of the main drives of innovations when the advanced sensors, various control systems, surveillance and reconnaissance drones, and satellite communication systems are concerned. Consequently, the defense sector is interested in adequate introduction of commercial communication and IoT solutions for its own purposes. However, the development of these is mainly driven by the private sector while the military often lags behind. Thus, adopting IoT-based solutions and business practices that satisfy the basic requirements of certain tactical systems, through partnerships with the private sector, presents an opportunity for defense and public safety

sectors. In scope of this, the comparison of basic technology stacks related to the defense and public safety sector with the private sector, as shown in Figure 2, can be of great interest in terms of possible IoT technology adoption.

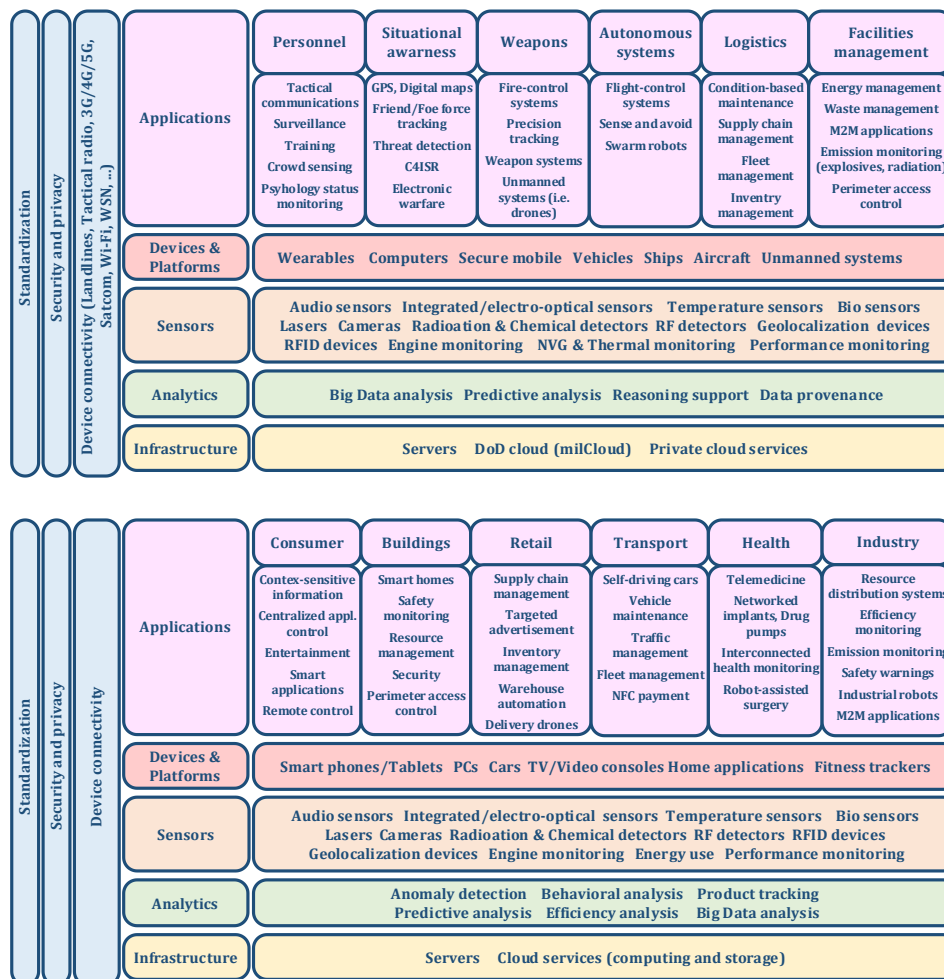


Figure 2 – The comparison of basic technology stacks suitable for the defense and public safety sectors (above) and for the private sector (under). Created by the authors based on (Fraga-Lamas et al, 2016)

Рис. 2 – Сравнение базовых технологических пакетов, подходящих для секторов обороны и общественной безопасности (сверху) и для частного сектора (снизу). Создано авторами на основе (Фрага-Ламас и др., 2016)

Слика 2 – Поређење основних технолошких пакета погодних за сектор одбране и јавне безбедности (изнад) и за приватни сектор (испод). Сачинили аутори на основу (Fraga-Lamas et al, 2016)

In addition to this introduction and conclusion section, the paper contains seven more sections. In the next section, the IoT architecture in the area of military technologies is described. The following sections describe the results and trends of research on the application of IoT in the areas of surveillance, target detection and threat localization, data collection and analysis for the purpose of aerospace forces, as well as in the area of monitoring health of soldiers and medical surveillance and logistics. A short summary of the paper is given in the concluding section.

General aspects of the IoT architecture for the support of military applications

The Internet of Things concept represents a revolution in the field of information technologies, and it creates fertile ground and enables special value for the application of artificial intelligence. Basically, the IoT concept assumes that everything can be connected and controlled using apps and sensors. IoT devices detect the observed phenomena and events through the sensor, collect data and forward it to the cloud for the further processing and analysis. Through the cloud, where the processing, analysis, controlling and decision-making entities are located, smart devices communicate with each other without the human intervention, which enables them to continuously learn (i.e. by employing machine learning) and implement their own solutions in the future. Obviously, all this presents an excellent basis for artificial intelligence. Given that there are a large number of devices that generate a huge amount of data, IoT technology is the driver of a special area, namely the analysis of Big Data in the real time.

However, although IoT systems connect a large number of heterogeneous devices, there is still no single standardized IoT system architecture.

The expansion of smart IoT devices creates new challenges for the cloud-based systems and cloud computing, especially because a large amount of data must be processed, particularly videos in real time, and the challenges related to the security and privacy. These problems are expressed both in humans and in devices intended for military applications. For this reason, the idea of applying federated learning (FL) as a privacy-preserving solution came up (Zhang et al, 2022). Federated learning for IoT implies that the raw data is not collected centrally but separately on each IoT device, thus protecting user's privacy since sensors can directly record data about users or devices. The idea of FL lies in the following: each IoT device processes the necessary amount of

data and forwards the finally extracted information through the network, whereby the raw data remains protected and does not leave the devices. Data processing through the use of artificial intelligence in the device itself can also be limited to the available data set, and for this reason, parallel learning between multiple devices and their mutual information exchange can be realized. In this way, the means to relieve the network resources is also created, which can be a limiting factor of the system, if not resolved, especially for low bandwidth IoT networks. However, several potential limitations have been identified for the full implementation of FL, which must be taken into account when these systems are designed and built. In the process of collecting and processing data on the device itself, there must be appropriate local resources that can support the collected data in terms of storage, handling and processing. The data transmission network must have adequate bandwidth so that there is no congestion or information delay in mutual communication between devices and communication with the central part of the system in the cloud. In a real environment, there is also a possibility that certain devices become temporarily absent from the network due to physical obstacles or malicious (i.e. enemy) attacks. However, the data handling capacities of various IoT devices are usually not uniform, and the dynamics of data distribution from individual devices is not uniform in the system. Thus, it is preferable to solve the mentioned potential problems during the system design and construction phase.

In the last few years, a lot of effort has been put into the research and development of IoT technology due to the need to improve military capabilities. In this effort, the one of the main task was created due to the fact that the generation of large amounts of data by IoT devices requires the protection of confidential data. Yet, blockchain technology allow IoT devices to exchange collected data with each other or send it to a cloud server safely and reliably (Fotia et al, 2023). Thus, blockchain-based solutions represents the decentralization of data storage, processing and distribution quickly and securely online without the need for a trusted authority. Given that in practice there is a need for both centralized and decentralized data storage, so-called hybrid blockchain platforms were developed, which achieved the existence of public and private blockchains in the same project, where anyone can access and view public data, and protected data cannot be accessed without the predefined permissions (Alkhateeb et al, 2022). Also, the hybrid blockchain platform is customizable so that the administrator can define which transactions will be public or who can participate in the specific blockchain. It should be also noticed that the research in this area

currently moves in several directions. The application of artificial intelligence for monitoring or control may have limitations in terms of energy efficiency, depending on the type of device. On the other hand, the interoperability requirements between two or more hybrid blockchains are not simple. Therefore, it is necessary to implement an effective mechanism of communication in order to simplify this process. Accordingly, data security for hybrid blockchains in IoT environments requires further research due to the existence of a broad range of sensitive and confidential data.

The military application of IoT technology is considered and developed in order to improve combat effectiveness and effective management of the resources. When IoT technology is used for defense applications it is often called the Internet of Battlefield Things (IoBT), (Wang et al, 2018b). In Internet of Battlefield Things, application requires the processing of a large amount of data, the validity and accuracy of which directly affect the quality of the military decision-making process. The existing architecture of data transmission and information on the battlefield is not able to support the current and future requirements of data collection and processing, which is why the IoBT has found its place and role in modern defense applications.

The first IoBT architecture was based on the data processing center placed in the cloud, the so-called "battle cloud", located far from the combat touch of tactical units. As such, it was highly susceptible to the communication congestion due to the bandwidth limitations and information transfer delays (i.e. end-to-end latency). Given that all data flows into one center, this center, as well as the associated communications links, would certainly become a target of attacks as such. Additionally, in practice there is a possibility of impairing the robustness of the data transmission network in case of deliberate attacks by the enemy due to the reduction of the number of one-way edges and nodes in the network (Feng et al, 2020). In order to overcome the mentioned problem, the idea of inserting another layer of the so-called "battle clouds-fog" came up (Bonomi et al, 2012; Hossain et al, 2019). However, due to heterogeneous equipment, load and delay in a distributed network, it is necessary to perform load balancing in order to allocate resources for assigned tasks, which is one of the important areas of the current research (Wang et al, 2018a).

The ability of IoT technology to create effects in the physical world through the use of actuators and other autonomous physical platforms enables management in the air, on the ground, at the sea and in the space through the cyber interfaces, using the intelligent command and

control (C2) (Russell et al, 2019). This means that the IoBT, in addition to provided help in the execution of the primary task, also makes valuable predictions and can suggest continuity in the action. These are integrated into the multi-dimensional environment through IoTs autonomous platforms, on the land, at the sea and in the air, with the intelligent command and control systems (C2), which ensure the execution of tasks and the fulfillment of the final desired state by enabling the monitoring of a wide range of human activities in a dynamic environment that the existing command and control systems are not able to provide (Russell & Abdelzaher, 2018). Due to the necessity to transfer a large amount of data, it is also necessary to build an appropriate telecommunications infrastructure that will support the C2 system. In that area, the research trend is the transfer of data from the still incompletely used 5G network capabilities to the new level of the 6G network (Qadir et al, 2023).

However, the question of the distribution of responsibilities between the commanders and the machines (devices) is also raised. Through the use of IoT technologies and C2 intelligent systems, a quick reconfiguration of forces and resources can be enabled in order to achieve the desired effect to satisfy the information the commander's needs to the unexpected resource losses or in the case of unfavorable land and weather environment (Abdelzaher et al, 2018a). This will certainly require changes in the operational concept, doctrine, tactics and structure of military units, which is the subject of further research in the subject area.

Decision making in the military systems is a hierarchical one and takes a certain amount of time. The needs of the practice are that this time should be as short as possible and the decision should be made in timely manner. Thus comes the need for a compromise between the delegation of decision-making authority and the predictability of risk, given that the higher level of delegation means the lower predictability level of aggregate behavior. The basic question how to design (place) the optimal solution between the human and an algorithm present one of the important directions of research in the subject area. IoT services will certainly contribute to a greater degree of automation and improvement of the quality of military decisions on the battlefield, especially in the conditions of unexpected scenarios in an unpredictable hostile environment, thus facilitating the reduction in both human and material losses in the operations. The main question to be considered here is the establishment of the relationship between reliability and artificial intelligence. A prerequisite for artificial intelligence is deployment of machine learning techniques, which inherently requires human-created

models of the specific environments. Therefore, in order to design the sensitive and safety-critical decisions, learning algorithms based on the deep neural networks are currently being researched, which must enable the flexibility of the structure that functions in an unknown environment and the generation of training and testing data in order to obtain guarantees, i.e. to manage risk (Abdelzaher et al, 2018b). Reducing the physical presence of a person in hostile environments and increasing the toughness of assets on the battlefield requires the necessary level of embedded intelligence able to detect and predict the behavior of the enemy, to define the necessary level of response to the threat, to properly adapt to sudden changes in the environment, to recover in case of attacks and losses, and to support continuous learning.

In the next several subsections, the most important IoT military application areas will be presented.

IoT-based surveillance applications

The IoT systems played a significant role in the field of surveillance and control of soldiers and units. The main characteristic of the so-called Military Assistance and Surveillance System (MASS) is to enable network-centric warfare, which requires linking individuals and units with unit command. As described in the paper (Raja & Bagwari, 2018), the MASS enables the reception and transmission of data, such as navigation elements, atmospheric conditions, state of health, command information, transmission of data from other devices (such as rangefinders) in real time, via a portable device with a user interface. In addition to these devices, the soldiers' equipment includes sensors for collecting data and recording the environment, and the transparent displays that allow the soldier to observe data in the form of augmented reality so that they do not require the soldier's attention to be diverted from the battlefield. In addition to the above, it is possible to connect several devices to the system, such as ammunition counters. With the help of the MASS, unit commanders have the ability to visualize the deployment of forces and to collect data independently of the engagement of individuals, which certainly makes it easier to make faster and better decisions related to the battlefield.

The application of IoT technology in the provision of smart cities through the services of traffic control, surveillance, management, police, etc., has also been transferred to the public security and defense sectors. Supervision and control of military facilities and facilities of importance for the national security is the application area of the systems in which

various data is collected and processed with the help of video cameras, microphones and various other sensors, while the protection and warning system are activated accordingly (Pahal et al, 2018). In practice, given that one sensor can detect a certain phenomenon under certain conditions, layering and synchronization of sensory data must be done in order to make more accurate decisions about the current state and the future activities. The system should also be capable of learning based on the past events, so that it can recognize false alarms and then performs modeling to predict the dynamic dependence between different entities in the overall picture. One important research direction in this area is the issue of smart reasoning and detection of image content in order to recognize a suspicious content (event) in real time.

One way to overcome the challenge related to the need to process a large amount of data in real time is based on the application of multilayer neural networks using the centralized (cloud) computing and the edge computing, as describe in (Zhao et al, 2019), where data is primarily processed at the edge devices and not on central servers. In this way, we can achieve significant savings in terms of deployed network resources, information delay is significantly reduced, and data leakage from source to source is prevented.

In the defense and security sector, the primary role is certainly played by the human itself, with his regulated characteristics and tendencies. However, that person must possess the required degree of integrity to perform important state and military affairs. Given that a person in his daily life does not carry out activities according to a checklist, but routinely performs many free activities, there is a possibility of non-intentional, and sometimes intentional, leakage of data and information of importance to the defense system. Preventing the outflow of confidential data and information is one of the areas of application of IoT (Fongen & Mancini, 2015) technology aimed at monitoring the various activities and behavior of personnel in the defense and security sector in their daily activities, with the aim of information leakage prevention. As an example, the terrorist attacks in Paris, India and the USA were possible due to security failures and the leakage of classified information through defense personnel (Bhatia & Sood, 2018), and it is concluded that the integrity of each individual directly affects national security.

The paper (Bhatia & Sood, 2018) presents a 4-phase IoT-based model for assessing staff activity. The proposed model is based on the collection of information on staff activities, analysis information and determining its integrity with regard to the national security. Activity

quantification is done in the form of determining the degree of integrity as an index that is compared with a defined value threshold. The proposed model was tested on multiple datasets and proved to be effective in terms of estimating the integral behavior of defense personnel. One of the research challenges in this area is the heterogeneity of input data, which would be a guideline for further research in the subject area.

Finally, one of the applications of IoT technology is the surveillance of robotic unmanned platforms used for military purposes (Telkar & Gadgay, 2020), such as aircraft, underwater and land vehicles. These platforms are equipped with sensors for detecting the primary target, such as mines, and other sensors for orientation, detection of atmospheric conditions, environmental imaging, etc. By recognizing the specific shape, the platform makes a decision about the upcoming action, movement, effect of weapons systems, etc. The primary data processing takes place on the crew platform, while the secondary processing takes place in the monitoring and supervision center. The application of the IoT concept on humanoid robots is particularly interesting, which is an area of interest for technologically developed countries.

Enemy localization and target detection

Locating the enemy on the battlefield is a question that is of great interest to commanders in order to direct forces and assets in combat operations. The collection of data on terrain, weather, the state of one's own units and the enemy through sensor networks has been discussed in several works (Akman et al, 2018). Data collection and location prediction was done through acoustic sensors and the application of the triangulation method as explained in (Sallai et al, 2011). There are also solutions for collecting data using helmet-mounted microphones which use time and angle of sound detection to determine the location of the enemy. However, data processing requirements have grown over time, such as to lower energy consumption, suppress echo signals, improve sensor calibration quality, increase detection distance, deploy information on weather conditions, etc. All these requirements took their toll, which is why most current and foreseen solution are switched to the IoT approach. Modern solutions also use micro electro-mechanical sensors (MEMS) which, among others, have GPS (Global Positioning System) receivers for determining the location of soldiers. The location of the enemy is determined according to the direction and direction of fire of own forces. Also, depending on the armament, laser rangefinders are used. The data is usually not processed at the source, but is distributed

to the application server where it is processed and returned to the user in the form of information, which creates the high demands related to the end-to-end delays.

Situation awareness

Military operations are carried out in complex environments which are highly dynamic and not quite predictable. The introduction of IoT technology significantly contributes to the exchange of data and information quality and makes it easier for commanders to make decisions and achieve a greater degree of efficiency (Michalski & Bernat, 2019). However, the integration of a large number of heterogeneous sensors for monitoring purposes contributes to the significant increase in the risk of cyber-attacks. Thus, the level of trust in incoming data presents an important challenge for researchers in this area (Glowacka et al, 2015). Certain entities in the network can become hostile, due to the capture by the enemy, and thus interfere with the operation of the network and the entire infrastructure. Therefore, given that wireless transmission is involved, special attention must be paid to the design and implementation of security mechanisms, encryption algorithms, secure routing protocols (especially due to entity mobility), and trust assessment. Trust assessment should be based on direct observations and received recommendations. Based on trust assessment, malicious and unintentional intrusions are detected and adequate measures are taken in order to prevent and eliminate threats. Trust assessment can be performed in several ways, such as: by direct monitoring (Sun et al, 2014), assessment based on received data, by weighting the evaluation function based on the history of entity behavior, or on the basis of exchange of certificates and risk assessment.

Air space applications

Airspace management requires strict coordination of aircraft by location and time in order to achieve the required level of flight safety. In combat operations, in addition to the own ones, the enemy aircraft of all types must be considered, while there is also the use of artillery armament, which additionally limits the corridors of movement for the own aircraft. Given that the use of enemy assets is stochastic in time, it is necessary to provide the pilot with the timely information about the regime and route of movement. The key limitations in the airspace management in the area of operations are (Singh et al, 2019):

- vertical separation, when aircraft have a low flight profile to avoid detection by the enemy,
- avoiding a collision with one's own armament during the over flight of one's own forces,
- avoiding collision with own aircraft, and
- unforeseen conflict with enemy aircraft.

Timely information, warning or command, is of crucial importance for pilots. Through the use of IoT technology, data collection, processing and distribution to interested parties, primarily pilots, will enable more efficient management of flight safety and overcoming most of the before mentioned problems. The processing of data collected from ground forces and air forces is performed centrally, in real time, so that the coordination of all subjects in the area of operation is enabled. Visualization of space through virtual or augmented reality, as part of suggestion of maneuvers process, will enable a new approach in solving highly demanding tactical situations in airspace.

Military health

A special field of application of the Internet of military things is the field of health care of soldiers. However, from justified works, the impact of electromagnetic radiation in the network itself on humans was also investigated (Nasim & Kim, 2019) where the research identified the safety distances of radiation sources necessary to maintain human health. In this area, the triage on the battlefield represents an extremely important task on which highly depends the degree of survival of soldiers due to wounds, injuries or illnesses. For this purpose, special sensors were developed with the task of collecting data on individuals in order to make proper decisions about the future treatment, namely Immediate Treatment, Delayed Treatment, Minimal Treatment or Expectant Treatment (Dyk et al, 2017). Besides the traditional triage on the battlefield, monitoring the health condition of soldiers in real time and responding to critical events in a timely manner has become particularly important (Reyes et al, 2017). For this reason, so-called medical networks are researched and developed, which should enable viable connections of devices and sensors from different sensor manufacturers, secure data transmission, the possibility of calling the call center for consultation, and also counseling between doctors in the field and specialists via telemedicine (Jarmakiewicz et al, 2016).

Another application of the IoT in military health is searching the terrain and finding the injured and sick soldiers, which, among other, requires special data transmission conditions to protect soldiers from the enemy. In addition to the requirements for authentication and biometrics of the soldiers, it is required that smart devices deployed possess enough energy to enable secure and reliable communication between soldiers and the nodes of the network, which must be maintained long enough, i.e. until the arrival of the care and evacuation team (Kang et al, 2020).

Military logistics

The application of the Internet of Things in military logistics has a very wide application in unifying logistical functional areas (supply, maintenance of weapons and military equipment, traffic and transport, quartermaster's office, healthcare, etc.) and in the realization of process functions (Zhong et al, 2012). The concept of network organization in the military logistics system is based on the organization of logistics system monitoring, and most often consists of several branches that monitor individual logistics functions due to different requirements in terms of data collection and analytic, as well as due to different ways of data generation (Wang et al, 2018a, Wei et al, 2012). In addition to collection, processing and distribution of data and information within the individual logistics functions, an important area of the application of the IoT is in the field of logistics of the asset itself. This enables the end user to initiate actions in order to preserve the operational capabilities of the weapon itself or mass service for a group of assets (Liang et al, 2014).

The construction of the logistics system is directly related to the construction of weapons. Project bureaus and institutes use so-called Product life-cycle management (PLM) software tools that enable connections at the national and international level with potential future manufacturers of the asset itself, manufacturers of components and spare parts, distributors, etc., for which the IoT infrastructure is necessary (Rondon et al, 2022).

Monitoring the flow of the production or the asset overhaul requires a very wide range of data and analytics to avoid downtime and to reduce business efficiency. For this purpose, IoT networks are being developed with the aim to monitor workforce capacity, consumption and demand for spare parts and consumables, energy, material distribution, work control and the entire quality system, etc. Since in many production plants these are realized manually, this actually presents the perfect area of the

application of the loBT in accordance with the visions of industry 4.0 (Salih et al, 2022).

For the successful management of weapons and military equipment in combat units, it is necessary to monitor the state of assets in real time, and to initiate maintenance activities in order to maintain the required level of operational availability of units. For this purpose, electronic identity cards of asset are being developed to record the state and status of particular assets, embedded computers inside equipment that collect and process data on the state of individual systems are deployed, as well as assemblies and parts which indicate a timely reaction to the user (Liu et al, 2022). For certain assets, devices are installed that alert the maintenance service in real time in order to shorten the response time in the so-called condition-based maintenance concept. Decision-makers in the function of maintenance and overhaul need timely knowledge about the state of maintenance capacity, both in the background and in the operational area, in the short term or for the operation as a whole.

Logistics personnel require information on the state of reserves of all classes of materials, the position of distributors, the movement of convoys, storage conditions, the possibility of delivery and evacuation of assets, the health status of personnel, etc. Finally, the question arises as to how to allocate logistics capacities for the optimal satisfaction of user needs in accordance with the place and role in combat operations. For such a thing, it is necessary to apply experiential and analytical tools of artificial intelligence based on multi-criteria decision making, which humans as individuals cannot do as successfully as machines do (Lei, 2022).

All the aforementioned areas are the ones in which modern armed forces invest significant resources in order to raise the level of effectiveness and efficiency of combat units based on loBT technology deployment.

Conclusion

The military application of IoT technology is considered and developed in order to improve combat effectiveness and effective management of the resources based on a large amount of data, the validity and accuracy of which directly affect the quality of the military decision-making process. The existing architecture of data transmission and information on the battlefield is not able to support the current and future requirements of data collection and processing, which is why the loBT has found its place and role in modern defense applications.

Given that all data flows into one center, such a center, as well as the associated communications links, would certainly become a target of attacks as such.

The ability of IoT technology to create effects in the physical world through the use of actuators and other autonomous physical platforms enables management in the air, on the ground, at the sea and in the space through cyber interfaces, using intelligent command and control. Due to the necessity to transfer a large amount of data, it is also necessary to build an appropriate telecommunications infrastructure that will support the C2 system. In that area, the research trend is the transfer of data from the still incompletely used 5G network capabilities to the new level of the 6G network.

Through the use of IoT technologies and C2 intelligent systems, the information needs of a commander can be satisfied in order to enable quick reconfiguration of forces and resources in response to unexpected resource losses or in case of unfavorable terrain and weather conditions. This will certainly require changes in the operational concept, doctrine, tactics and structure of military units, which is the subject of further research in the subject area.

References

Abdelzaher, T., Ayanian, N., Basar, T., Diggavi, S., Diesner, J., Ganesan, D., Govindan, R., Jha, S., Lepoint, T., Marlin, B., Nahrstedt, K. et al. 2018a. Toward an Internet of Battlefield Things: A Resilience Perspective. *Computer*, 51(11), pp.24-36. Available at: <https://doi.org/10.1109/MC.2018.2876048>.

Abdelzaher, T., Ayanian, N., Basar, T., Diggavi, S., Diesner, J., Ganesan, D., Govindan, R., Jha, S., Lepoint, T., Marlin, B., Nahrstedt, K. et al. 2018b. Will Distributed Computing Revolutionize Peace? The Emergence of Battlefield IoT. In: *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, Vienna, Austria, pp.1129-1138, July 02-06. Available at: <https://doi.org/10.1109/ICDCS.2018.00112>.

Akman, Ç., Sönmez, T., Özüğür, Ö., Başlı, A.B. & Kemal Leblebicioğlu, M. 2018. Sensor fusion, sensitivity analysis and calibration in shooter localization systems. *Sensors and Actuators A: Physical*, 271, pp.66-75. Available at: <https://doi.org/10.1016/j.sna.2017.12.042>.

Alkhateeb, A., Catal, C., Kar, G. & Mishra, A. 2022. Hybrid Blockchain Platforms for the Internet of Things (IoT): A Systematic Literature Review. *Sensors*, 22(4), art.number:1304. Available at: <https://doi.org/10.3390/s22041304>.

Bhatia, M. & Sood, S.K. 2018. Internet of Things based activity surveillance of defence personnel. *Journal of Ambient Intelligence and Humanized Computing*, 9, pp.2061-2076. Available at: <https://doi.org/10.1007/s12652-017-0507-3>.

Bonomi, F., Milito, R., Zhu, J. & Addepalli, S. 2012. Fog computing and its role in the internet of things. In: *MCC '12: Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, Helsinki, Finland, pp.13-16, August 17. Available at: <https://doi.org/10.1145/2342509.2342513>.

Dyk, M., Chmielewski, M. & Najgebauer, A. 2017. Combat triage support using the Internet of Military Things. In: *2017 Federated Conference on Computer Science and Information Systems (FedCSIS)*, Prague, Czech Republic, pp.835-842, September 03-06 [online]. Available at: <https://ieeexplore.ieee.org/abstract/document/8104646> [Accessed: 5 March 2023].

Feng, Y., Li, M., Zeng, C. & Liu, H. 2020. Robustness of Internet of Battlefield Things (IoBT): A Directed Network Perspective. *Entropy*, 22(10), art.number:1166. Available at: <https://doi.org/10.3390/e22101166>.

Fongen, A. & Mancini, F. 2015. Integrity attestation in military IoT. In: *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Milan, Italy, pp.484-489, December 14-16. Available at: <https://doi.org/10.1109/WF-IoT.2015.7389102>.

Fotia, L., Delicato, F. & Fortino, G. 2023. Trust in Edge-based Internet of Things Architectures: State of the Art and Research Challenges. *ACM Computing Surveys*, 55(9), pp.1-34. Available at: <https://doi.org/10.1145/3558779>.

Fraga-Lamas, P., Fernández-Caramés, T.M., Suárez-Albela, M., Castedo, L. & González-López, M. 2016. A Review on Internet of Things for Defense and Public Safety. *Sensors*, 16(10), art.number:1644. Available at: <https://doi.org/10.3390/s16101644>.

Głowacka, J., Krygier, J. & Amanowicz, M. 2015. A trust-based situation awareness system for military applications of the internet of things. In: *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Milan, Italy, pp.490-495, December 14-16. Available at: <https://doi.org/10.1109/WF-IoT.2015.7389103>.

Hossain, M.S., Ramli, M.R., Lee, J.M. & Kim, D.-S. 2019. Fog Radio Access Networks in Internet of Battlefield Things (IoBT) and Load Balancing Technology. In: *2019 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, Korea (South), pp.750-754, October 16-18. Available at: <https://doi.org/10.1109/ICTC46691.2019.8939722>.

Jarmakiewicz, J., Parobczak, K. & Maślanka, K. 2016. On the Internet of Nano Things in healthcare network. In: *2016 International Conference on Military Communications and Information Systems (ICMCIS)*, Brussels, Belgium, pp.1-6, May 23-24. Available at: <https://doi.org/10.1109/ICMCIS.2016.7496572>.

Kang, J.J., Yang, W., Dermody, G., Ghasemian, M., Adibi, S. & Haskell-Dowland, P. 2020. No Soldiers Left Behind: An IoT-Based Low-Power Military

Mobile Health System Design. *IEEE Access*, 8, pp.201498-201515. Available at: <https://doi.org/10.1109/ACCESS.2020.3035812>.

Lei, N. 2022. Intelligent logistics scheduling model and algorithm based on Internet of Things technology. *Alexandria Engineering Journal*, 61(1), pp.893-903. Available at: <https://doi.org/10.1016/j.aej.2021.04.075>.

Liang, F., Bai, H.W. & Liu, G.D. 2014. Application of internet of things in military equipment logistics. *Applied Mechanics and Materials*, 556-562, pp.6723-6726. Available at: <https://doi.org/10.4028/www.scientific.net/AMM.556-562.6723>.

Liu, C., Su, Z., Xu, X. & Lu, Y. 2022. Service-oriented industrial internet of things gateway for cloud manufacturing. *Robotics and Computer-Integrated Manufacturing*, 73, art.number:102217. Available at: <https://doi.org/10.1016/j.rcim.2021.102217>.

Michalski, D. & Bernat, P. 2019. Internet of Things in Air and Missile Defence A System Solution Concept. In: *2019 International Conference on Military Technologies (ICMT)*, Brno, Czech Republic, pp.1-5, May 30-31. Available at: <https://doi.org/10.1109/MILTECHS.2019.8870070>.

Nasim, I. & Kim, S. 2019. Human EMF Exposure in Wearable Networks for Internet of Battlefield Things. In: *MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM)*, Norfolk, VA, USA, pp.1-6, November 12-14. Available at: <https://doi.org/10.1109/MILCOM47813.2019.9020889>.

Pahal, N., Mallik, A. & Chaudhury, S. 2018. An Ontology-based Context-aware IoT Framework for Smart Surveillance. In: *SCA '18: Proceedings of the 3rd International Conference on Smart City Applications*, Tetouan, Morocco, art.number:69, pp.1-7, October 10-11. Available at: <https://doi.org/10.1145/3286606.3286846>.

Pokorni, S.J. 2019. Reliability and availability of the Internet of things. *Vojnotehnički glasnik/Military Technical Courier*, 67(3), pp.588-600. Available at: <https://doi.org/10.5937/vojtehg67-21363>.

Qadir, Z., Le, K.N., Saeed, N. & Munawar, H.S. 2023. Towards 6G Internet of Things: Recent advances, use cases, and open challenges. *ICT Express*, 9(3), pp.296-312. Available at: <https://doi.org/10.1016/j.ict.2022.06.006>.

Raja, P. & Bagwari, S. 2018. IoT Based Military Assistance and Surveillance. In: *2018 International Conference on Intelligent Circuits and Systems (ICICS)*, Phagwara, India, pp.340-344, April 19-20. Available at: <https://doi.org/10.1109/ICICS.2018.00076>.

Reyes, Ch.R.P., Vaca, H.P., Calderón, M.P., Montoya, L. & Aguilar, W.G. 2017. MilNova: An approach to the IoT solution based on model-driven engineering for the military health monitoring. In: *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*, Pucon, Chile, pp.1-5, October 18-20. Available at: <https://doi.org/10.1109/CHILECON.2017.8229585>.

Rondon, L.P., Babun, L., Aris, A., Akkaya, K. & Uluagac, A.S. 2022. Survey on enterprise Internet-of-Things systems (E-IoT): A security perspective. *Ad Hoc*

Networks, 125, art.number:102728. Available at: <https://doi.org/10.1016/j.adhoc.2021.102728>.

Russell, S. & Abdelzaher, T. 2018. The Internet of Battlefield Things: The Next Generation of Command, Control, Communications and Intelligence (C3I) Decision-Making. In: *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, Los Angeles, CA, USA, pp.737-742, October 29-31. Available at: <https://doi.org/10.1109/MILCOM.2018.8599853>.

Russell, S., Abdelzaher, T. & Suri, N. 2019. Multi-Domain Effects and the Internet of Battlefield Things. In: *MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM)*, Norfolk, VA, USA, pp.724-730, November 12-14. Available at: <https://doi.org/10.1109/MILCOM47813.2019.9020925>.

Salih, K.O.M., Rashid, T.A., Radovanovic, D. & Bacanin, N. 2022. A comprehensive survey on the Internet of Things with the industrial marketplace. *Sensors*, 22(3), art.number:730. Available at: <https://doi.org/10.3390/s22030730>.

Sallai, J., Lédeczi, A. & Völgyesi, P. 2011. Acoustic shooter localization with a minimal number of single-channel wireless sensor nodes. In: *SenSys '11: Proceedings of the 9th ACM Conference on Embedded Networked Sensor Systems*, Seattle, Washington, pp.96-107, November 1-4. Available at: <https://doi.org/10.1145/2070942.2070953>.

Singh, K., Tripathi, G., Chullai, G.A., Kumar, J. & Kumar, P. 2019. Future Battlefield Air Space Management: An Internet of Things (IoT) Based Framework. In: *2019 International Conference on Signal Processing and Communication (ICSC)*, Noida, India, pp.15-21, March 7-9. Available at: <https://doi.org/10.1109/ICSC45622.2019.8938280>.

Sun, Z.F., Ma, X. & Sun, D.X. 2014. Construction of the Air Offensive Operation Battlefield Support System based on the Internet of Things Technology. *Advanced Materials Research*, 834-836, pp.1873-1876. Available at: <https://doi.org/10.4028/www.scientific.net/AMR.834-836.1873>.

Telkar, A.K. & Gadgay, B. 2020. IoT Based Smart Multi Application Surveillance Robot. In: *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, pp.931-935, July 15-17. Available at: <https://doi.org/10.1109/ICIRCA48905.2020.9183289>.

Vermesan, O. & Friess, P. (Eds.) 2014. *Internet of Things Applications - From Research and Innovation to Market Deployment, 1st edition*. New York: River Publishers. Available at: <https://doi.org/10.1201/9781003338628>.

Wang, J., Cao, L., Shen, Y. & Zheng, G. 2018a. Research on Design of Military Logistics Support System Based on IoT. In: *2018 Prognostics and System Health Management Conference (PHM-Chongqing)*, Chongqing, China, pp.829-832, October 26-28. Available at: <https://doi.org/10.1109/PHM-Chongqing.2018.00148>.

Wang, Y., Ren, Z., Zhang, H., Hou, X. & Xiao, Y. 2018b. "Combat Cloud-Fog" Network Architecture for Internet of Battlefield Things and Load Balancing Technology. In: *2018 IEEE International Conference on Smart Internet of Things*

(SmartIoT), Xi'an, China, pp.263-268, August 17-19. Available at: <https://doi.org/10.1109/SmartIoT.2018.00054>.

Wei, X., Wan, Y., Ding, H. & Xu, H. 2012. Conception of Intelligent Military Logistics Based on Internet of Things Technology. In: *ICLEM 2012: Logistics for Sustained Economic Development—Technology and Management for Efficiency*, Chengdu, China, pp.371-375, October 8-10. Available at: <https://doi.org/10.1061/9780784412602.0059>.

Zhang, T., Gao, L., He, C., Zhang, M., Krishnamachari, B. & Avestimehr, A.S. 2022. Federated learning for the internet of things: Applications, challenges, and opportunities. *IEEE Internet of Things Magazine*, 5(1), pp.24-29. Available at: <https://doi.org/10.1109/IOTM.004.2100182>.

Zhao, Y., Chen, Q., Cao, W., Jiang, W. & Gui, G. 2019. Deep Learning Based Couple-like Cooperative Computing Method for IoT-based Intelligent Surveillance Systems. In: *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Istanbul, Turkey, pp.1-4, September 08-11. Available at: <https://doi.org/10.1109/PIMRC.2019.8904229>.

Zhong, X.-H., Ding, H., Zhang, X.-M. & Zhang, F. 2012. Research on the Construction of the IOT System in the Field of Military Logistics. In: *ICLEM 2012: Logistics for Sustained Economic Development—Technology and Management for Efficiency*, Chengdu, China, pp.376-382, October 8-10. Available at: <https://doi.org/10.1061/9780784412602.0060>.

Zhu, L., Majumdar, S. & Ekenna, C. 2021. An invisible warfare with the internet of battlefield things: A literature review. *Human behavior and emerging technologies*, 3(2), pp.255-260. Available at: <https://doi.org/10.1002/hbe2.231>.

Интернет вещей в военном применении

Влада С. Соколович^а, корреспондент, Горан Б. Маркович^б

^а Университет обороны в г. Белград, Военная академия, Департамент логистики, Белград, Республика Сербия

^б Белградский университет, факультет электротехники, г. Белград, Республика Сербия

РУБРИКА ГРНТИ: 47.01.29 Информационная деятельность

ВИД СТАТЬИ: обзорная статья

Резюме:

Введение/цель: Термин „Интернет вещей“ (IoT) обычно относится к корпоративной сети подключенных устройств и технологии, которая облегчает связь между этими устройствами и облаком, а также между самими устройствами. Концепция Интернета вещей в последнее время рассматривается и применяется как при проектировании систем, предназначенных для распределения данных и информации между разнородными устройствами с целью

повышения эффективности деятельности и принятия решений. Интернет вещей обеспечивает мониторинг энергетики и цепочек поставок, координацию производства, оптимизацию производительности оборудования, транспортировку, здравоохранение, а также улучшает охрану труда и повышает безопасность. В дополнение к интеллектуальным устройствам технология Интернета вещей также позволяет подключать различные датчики в качестве источника данных о различных физических явлениях. Таким образом, основываясь на полученной информации, можно управлять работой устройств, делать прогнозы, принимать решения и пр. В данной статье анализируются конкретные области применения Интернета вещей в секторе обороны и безопасности с целью выявления возможностей применения современных технологий в повышении оборонного потенциала государства и определения направлений будущих исследований в предметной области.

Методы: В данной статье были применены методы контент-анализа текущих исследований, а затем с помощью дедуктивного метода были сделаны выводы о будущих направлениях развития технологии Интернета вещей

Результаты: Был проведен детальный анализ предыдущих и текущих исследований в секторе обороны и безопасности, а также даны потенциальные направления будущих исследований в области Интернета вещей с целью повышения оперативных возможностей вооруженных сил.

Выводы: Сервис Интернета вещей, безусловно, будет способствовать большей степени автоматизации и повышению качества военных решений на поле боя, особенно в условиях неожиданных сценариев в непредсказуемой вражеской среде, способствуя тем самым снижению как человеческих, так и материальных потерь в ходе военных действий.

Ключевые слова: интернет вещей, общественная безопасность и защита населения, приложения интернета вещей, локализация и обнаружение целей, военная логистика.

Интернет ствари у војној примени

Влада С. Соколовић^а, аутор за преписку, Горан Б. Марковић^б

^а Универзитет одбране у Београду, Војна академија, Катедра логистике, Београд, Република Србија

^б Универзитет у Београду, Електротехнички факултет, Београд, Република Србија

ОБЛАСТ: телекомуникације, информационе технологије
КАТЕГОРИЈА (ТИП) ЧЛАНКА: прегледни рад

Сажетак:

Увод: Појам интернет ствари (ИС) најчешће се односи на свеукупну мрежу повезаних уређаја и технологија која погодује комуникацији између ових уређаја и централних елемената мреже у „облаку” (cloud), као и између ових уређаја. Концепт ИС се од недавно разматра и примењује као адекватан за развој система чија је намена размена података и информација између хетерогених уређаја ради унапређења ефикасности и ефективности пословања и доношења одлука. Интернет ствари омогућава праћење енергије и ланца снабдевања, координацију производње, оптимизацију перформанси опреме, транспорт, јавно здравље и побољшава безбедност и здравље радника. Поред паметних уређаја, ИС технологија омогућава и повезивање различитих сензора као извора података о различитим физичким појавама, а на основу добијених информација могуће је контролисати рад уређаја, предвиђати, доносити одлуке, итд. Анализирају се специфичне области примене ИС у сектору одбране и безбедности, како би се идентификовале могућности примене савремених технологија у подизању одбрамбеног потенцијала државе и дефинисали правци будућих истраживања. Методе: Примењене су методе анализе садржаја актуелних истраживања, а затим су дедуктивном методом донети закључци о будућим правцима развоја ИС технологије.

Резултати: Извршена је детаљна анализа досадашњих и текућих истраживања у сектору одбране и безбедности и предложени потенцијални правци будућих истраживања ИС ради повећања оперативних способности оружаних снага.

Закључак: Услуге интернет ствари ће свакако допринети већем степену аутоматизације и побољшању квалитета војних одлука на бојном пољу, посебно у условима неочекиваних сценарија у непредвидивом непријатељском окружењу. Тиме ће се смањити људски и материјални губици у операцијама.

Кључне речи: интернет ствари, одбрана и јавна безбедност, апликације за интернет ствари, локализација и детекција циљева, војна логистика.

Paper received on / Дата получения работы / Датум пријема чланка: 09.03.2023.
Manuscript corrections submitted on / Дата получения исправленной версии работы /
Датум достављања исправки рукописа: 28.11.2023.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум
коначног прихватања чланка за објављивање: 29.11.2023.

© 2023 The Authors. Published by *Vojnotehnički glasnik / Military Technical Courier* (www.vtg.mod.gov.rs, втг.мо.упр.срб). This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Авторы. Опубликовано в «Военно-технический вестник / *Vojnotehnički glasnik / Military Technical Courier*» (www.vtg.mod.gov.rs, втг.мо.упр.срб). Данная статья в открытом доступе и распространяется в соответствии с лицензией «Creative Commons» (<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Аутори. Објавио Војнотехнички гласник / *Vojnotehnički glasnik / Military Technical Courier* (www.vtg.mod.gov.rs, втг.мо.упр.срб). Ово је чланак отвореног приступа и дистрибуира се у складу са Creative Commons лиценцом (<http://creativecommons.org/licenses/by/3.0/rs/>).

