10.26411/83-1734-2015-1-53-8-22

Security of ICT Networks for Logistics

Mariusz Frączek
Pomeranian University in Słupsk, Poland

Abstract
The overview study contains the most important issues decisive for ensuring the security of logistics ICT networks in the context of contemporary threats, at the same time bearing in mind their military dimension. It highlights the determinants influencing the functioning of the networks used to transmit information. The aspect of the need to ensure the protection of ICT networks dedicated to logistics has not been presented in this approach so far. The author first of all compares economic and hierarchical organizations based on the example of the armed forces. He also referred to the ICT networks of logistics of other uniformed formations.

Keywords: logistics, ICT network, threats, network security.

1. INTRODUCTION

The functioning of any organization, regardless of its purpose and nature, requires having strictly defined resources of equipment, devices and people who use them for variously defined purposes. It is estimated that such an approach is the foundation for the implementation of activities by every logistic system, regardless of its size. On the other hand, the efficiency and reliability of modern logistics, in the era of the information society, is inherently related to the possibility of using

modern ICT networks, thanks to which it has the ability to collect, process and transmit information, primarily in a digitized form. It is also worth noting that all documents with a classic form of presentation (e.g. paper / pictures / photos) are gradually converted to digital form. This constitutes a number of challenges faced by the persons managing (in charge) and responsible for the proper implementation of all undertakings that determine the success of activities undertaken by a given organization. Taking into account the numerous challenges and the possessed potential, the conclusion can be drawn that the above-mentioned ICT network is a specific bloodstream that can decide about 'to be or not to be' of any organization. Hence, the author estimates that in the 21st century its security is particularly important, bearing in mind that every institution, enterprise or company has information that may become desirable, regardless of whether it is considered secret (classified) or public, but they may be decisive for the success of marketing activities and its existence in the world of business or politics. It should also be noted that logistics in its genesis for many centuries of history was related to the implementation of tasks by the army and originally refers to strictly defined hierarchical structures. This also meant that currently, when we talk about logistics, the vast majority of us focus on rationality and pragmatic behaviour based on proven and good practices.

The area of scientific considerations formulated in this way was the foundation of the author's research and was explored to answer the main research problem formulated in the form of the question: ***what are the threats and how can the security of ICT networks of broadly understood logistics be ensured?***

The scope of the theoretical research carried out meant that the author's considerations presented in the further part of the study constitute not only a review of the literature on the subject, but also conclusions from his personal professional experience relating to both logistics and the ICT network. This is of particular importance after February 24, 2022, when the Central European region, once again in its history, after 77 years of peace, experiences a shock of warfare against our eastern neighbour, Ukraine. The above has re-evaluated the security of logistics ICT networks also in the context of contemporary military threats.

2. LOGISTICS AND ICT NETWORKS – THE ETYMOLOGICAL OVERVIEW

According to the author, there are no clear criteria describing how to ensure the security of the logistics ICT network in an organization. This is undoubtedly indicated by a number of factors of different nature that should be taken into account. On the other hand, its managers, thanks to the synergy of their activities, strive to achieve the desired goals set in logistics. As a result, the author considered it appropriate to refer to the propaedeutics concerning the functioning of logistics and ICT networks.

While studying the literature on the subject, one can encounter numerous definitions of the term „logistics". Their multitude and variety of interpretations made it difficult to present it unequivocally. The etymological roots of this concept are related to the words of Greek, English and French and, above all, mean[1]:

- logistikos - group rational;
- logistikon - group strength of reason (reason);
- logistics - gr. the art of calculating (counting);
- logos - gr. word, mind, counting,
- logistikas - Latin. providing the army with livelihoods;
- logistics and logistical - supply,
- logger, logis and logistique - fr. live, lodge.

Among the most popular interpretations of the definition of the term „logistics" it was assumed that *it is the process of planning, implementing and controlling the efficient and economically effective flow of raw materials, materials, finished products and relevant information from the point of origin to the point of consumption in order to meet customer requirements*[2].

The above references to definitions emphasize directly and indirectly the power of reason, prudence, common sense, the art of calculation (and counting), as well as expose the subject of logistics and knowledge about it. This proves that its impact should be perceived both in the conceptual sphere and in the practical sphere, i.e. the implementation of a number of broadly understood works, tasks, as well as projects constituting logistics activities. It is also worth noting and defining the essential features that are attributed to logistics, the most important of which are

[1] https://sites.google.com/site/historialogistyki/home/etymologia-logistyki, [Access on: 24.03.2022].

[2] https://pl.wikipedia.org/wiki/Logistyka [Access on: 24.03.2022].

presented below:

- planning and preparation of sourcing deliveries;
- planning and implementation of the provision of all services (including specialist);
- the field of knowledge of supply management;
- is currently a specialty within the scientific discipline of security science and economics and finance in the field of social sciences, which studies all dependencies regarding the planning, preparation, use and exchange of resources, people, information and services in order to achieve the desired benefits;
- includes customer service, demand forecasting, information flow, inventory control, order fulfilment, repair and overhaul, and parts supply;
- treated as a system - it is a set of forces and means that continuously carry out projects and tasks ensuring the effective functioning of all organizations, with particular emphasis on the needs of companies and enterprises, including the creation of optimal conditions for the production, storage and distribution of all necessary and luxurious goods.

Logistics activities may include (but do not have to be limited to them): customer service, demand forecasting, information flow, inventory control, handling, order fulfilment, repairs and parts procurement, location of production plants and warehouses, procurement processes, packaging, handling returns, waste management, transport and storage[3].

The author estimates that the possibilities of the functioning of a given organization (enterprise) and its development abilities depend to a large extent on the implemented and used ICT networks, which, among other things, is related to the constant search for the latest technologies and their implementation into the already existing systems supporting the logistics management of enterprises, companies, but also institutions related to the security of the state and its citizens.

Nowadays, there are over a dozen definitions that directly refer to ICT networks. Colloquially, during their characterization, a lot is written about the second part of the name, i.e. computer science, treating its first part (i.e. the prefix - „tele") as redundant. The fact is, however, that without it, no services would be provided, because it is impossible to use computers without a telecommunications infrastructure. Thus, the modern ICT network is a technically coordinated connection of telecommunications (transmission) networks with IT networks in the area of

[3] https://pl.wikipedia.org/wiki/Logistyka [Access on: 24.03.2022].

increasing the ability to exchange and transmit information (data) along with the constantly progressing convergence of various services.

The first element of the ICT network is telecommunications, the essence of which is the transmission of messages over long distances. The criteria for dividing telecommunications according to the type of connection set up are as follows:

- connection-oriented networks - prior to the commencement of information exchange, a connection is made, an example being PSTN (Public Switch Telecommunication Network) and GSM cellular network (Global System Mobile);
- connectionless networks - sending the information is not preceded by a connection commutation, while the recipient's address is at the beginning of the message and it is uncertain whether the recipient is available. An example is packet switching.

The criteria for dividing telecommunications according to the type of transmission medium are networks:

- wireless (radio, microwave);
- cable (wired, optical).

The second part of the ICT network is the IT network, which, in the greatest simplification, is based on computer networks with their end devices, the main purpose of which is the broadly understood ability to transmit data. It should be emphasized that, similarly to telecommunications, the literature on the subject presents information networks as a set of interrelated elements, the function of which is to process data using modern computer technology. It is called an IT system and its elements are presented below:

1. Equipment:
   - data storage devices (computer, laptop, netbook, tablet, but also a mobile phone);
   - devices for communication between hardware components of the system, and between people and information technology;
   - devices used to receive data - for example, electronic sensors, cameras, video recorders or scanners;
   - devices used for influencing the external environment by information systems, including through drivers of mechanical devices;
   - non-computer data processing devices (e.g. thermomix, smart refrigerator, smartwatch).
2. Software - system and utility.

3. Personal resources - users, service providers and technicians.
4. Organizational elements, i.e. all procedures related to the rules of using a given IT system, e.g. instructions, security policies, etc.
5. Information elements: domain (specialized) databases used by the IT system.

Another, much broader concept related to the transmission of information is an ICT system, which is defined *as a set of cooperating IT devices and software, ensuring processing and storage, as well as sending and receiving data via telecommunications networks using a terminal device appropriate for a given type of network*[4]. The ICT system is also an organizational and technical connection of various, often heterogeneous, ICT networks.

The author deems it appropriate to present the structure of the ICT network in a general manner. Only then can it be assessed its importance in terms of having the ability to provide comprehensive information exchange services for logistics purposes. It includes the interpenetrating elements and services of the following networks:

- telecommunications (transmission) network, which includes:
  - radio network (VHF / KF) - the devices used are: radios (narrow- and broadband, radiotelephones (including CB Radio - Citizen Band Radio);
  - radio-cable network (radio lines / cables);
  - cable network (copper / optical wires);
  - radio access network - separated as a service (radio stations / radiotelephones / GSM network);
  - satellite networks - separated as services (including radio communication / television / GPS navigation);
- computer network (wired or wireless - mainly Wi-Fi / Wimax / Bluetooth), which includes local and wide area computer networks.

ICT networks constitute the technical infrastructure for the communication system of each country, thanks to which all organizations have the ability to transmit any form of information. The other two (postal network and signalling network) are treated as alternative and will be valid in the event of a power failure in the ICT network. It should be noted that the basic elements that make up the modern ICT network are:

- tele-transmission infrastructure,
- telecommunication elements (devices),

[4] Act of 18 July 2002 on the provision of electronic services, OJ 2002, no. 144, item 1204.

- IT elements (devices),
- system applications (software),
- technical staff and system users.

It should be emphasized that the term „infrastructure" has a multifaceted meaning for logistics. And it's not just about data and message transfer. *In this approach, infrastructure means the foundation of the base, the necessary basis of the economy. This term is also used to describe all basic devices and institutions necessary for the proper functioning of the economy*[5]*. Infrastructure is also understood as devices serving the production sphere of the population through various types of services*[6].

A broader approach to the issue indicates that the technical infrastructure includes devices that allow to provide services in the field of communication, transport, energy, but also devices related to the regulation of rivers or environmental protection. Therefore, the technical infrastructure also includes:

- water supply;
- electricity supply;
- thermal energy supply;
- gas supply;
- expensive;
- waste disposal;
- telecommunications[7].

It was also considered appropriate to present three basic criteria for the classification of technical infrastructure:

1. Spatial scope (local, regional, national and international).
2. Impact on the location of production (special purpose, general purpose).
3. Property (own, general or personal, institutional, material)[8].

---

5 Rydzkowski W., *Usługi logistyczne*, Instytut Logistyki i Magazynowania, Poznań 2004.

6 Winiarski B. (red.), *Polityka gospodarcza,* Wydawnictwo Naukowe PWN, Warszawa 2004.

7 Obarska-Bartmańska M. et al., *Zasady lokalizowania i kształtowania przestrzennego zakładów i zespołów przemysłowych na przykładzie wybranych branż*, Instytut Kształtowania Środowiska, Warszawa 1986.

8 Witkowski K., *Zarządzanie infrastrukturą logistyczną gminy*, [in:] *Wybrane zagadnienia logistyki stosowanej*, Wydawnictwo Polskiej Akademii Nauk, Kraków 2005.

The technical infrastructure performs *(...) the function of servicing all production and service departments of the entire economy, integrating all its parts, and also provides conditions for the efficient functioning of the country*[9].

In the author's assessment, there is no doubt that the structure and functioning of an ICT network illustrated in such a way, together with its connections, allows to obtain a broader picture of the possibility of transmitting information in relation to a larger whole.

3. ICT NETWORKS FOR LOGISTICS – SELECTED EXAMPLES

In the 21st century, no one should deny that the information collected, processed and transferred for the purposes of logistics is important, for example, from the perspective of the functioning of any organization. The theory and practice also apply to the areas of interest of logistics ICT networks. The most important ones include production, storage, procurement, transport, sales (sales) and the collection of data on demand and supply, both for the local, regional, national and international market. In the latter case, there is a need to know the customs regulations in force in the territory of a given country or the European Union (NATO). An effectively operating information system in an organization is one of the key factors influencing the possibility of gaining a lasting advantage, regardless of whether it is a market for a specific product or in relation to the needs of hierarchical institutions. The infrastructure of the Logistics Information System consists of the following elements:

1. The technique of electronic documentation exchange - EDI (Electronic Data Interchange).
2. The technique of automatic identification AI - applies bar code reading - data identification using radio frequencies - RFID (Radio Frequency Identification), label printers.
3. Fixed telecommunications infrastructure - fixed telephony, PKP telephony, Netia, Orange telephony, telecommunications networks of cable television operators (UPC / Vectra), telecommunications networks for the needs of the Ministry of National Defense and the Ministry of Interior and Administration, as well as Internet service providers.
4. Mobile radio communication systems - GSM cellular networks (LTE and UMTS technologies) and satellite links, e.g. Inmarsat (International Maritime Satellite

[9] Fierla I. (red.), *Geografia gospodarcza Polski*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2004.

Organization), Globalstar, TS2 SPACE or Iridium, which is a commercial satellite cellular network that allows you to connect to another subscriber without ground station share.
5. Global Positioning System (GPS) navigation of mobile objects.

The effectiveness of the use of a logistic IT system depends primarily on the collection and input of accurate and confirmed data delivered in the shortest possible time. Their quality and number of entered into the system determines how the system will function, with what strength it will meet the expectations of functional persons (managers / managers / commanders), allowing for faster and effective decisions. Their use in the right place and time is currently the fundamental principle of „Just in time". It allows for the desired focus of the logistics effort.

The author is convinced that in the further part of the study, selected examples of IT solutions for logistics management used in various organizations (including hierarchical ones) should be presented, bearing in mind that it is only a representative group:
1. Organizations, corporations, enterprises, companies of an economic nature:
   - ADC (Automated Data Collection) - which includes automatic data identification (usually by barcodes) and transferring them to the IT system for further processing[10];
   - B2B (Business to Business) - "business-business" applications supporting transactions with the use of the Internet between enterprises[11];
   - B2C (Business to Consumer) – "business-consumer" applications supporting transactions using the Internet means the relationship between enterprises and customers[12,13];
   - BOM (Bill of Material) - is the management of the structure (structural connections) of products; it is a list of raw materials, components, parts and the amount of each of them needed to produce the final product[14].
   - DSS (Decision Support Systems) - IT systems supporting decision making based on large amounts of data collected over many years and numerous control parameters[15];

[10] https://www.logistyka.net.pl/slownik-logistyczny/szczegoly/4,adc [Access on: 25.03.2022].
[11] https://pl.wikipedia.org/wiki/B2B [Access on 25.03.2022].
[12] https://www.logistyka.net.pl/slownik-logistyczny/szczegoly/44,b2c [Access on: 25.03.2022].
[13] https://www.karierawfinansach.pl/baza-wiedzy/slownik-pojec/b2c-co-to-znaczy-b2c [Access on: 25.03.2022].
[14] https://www.system-kanban.pl/definicja/bom-bill-of-materials/ [Access on: 25.03.2022].
[15] Majewski J., *Informatyka dla logistyki*, Instytut Logistyki i Magazynowania, Poznań 2008, p. 51.

- CLS (Concurrent Logistics System) - definition of future IT systems based on ERP, ERM, using all possibilities of communication with a client and consumer, which support all possible scenarios of information exchange in order to meet the logistic needs of the company[16];
- CRM (Customer Relationship Management) - IT systems used to manage customer relations[17];
- CRP (Capacity Requirement Planning) – 'part' of the ERP system responsible for calculations related to the planning of production capacity loads[18];
- ECS - Export Control System[19];
- EDI (Electronic Data Interchange) - electronic exchange of standardized messages between IT systems[20];
- EIS (Executive Information Systems) - a system of informing top management, in which applications provide the company's management with reports and summaries from the DSS system[21];
- ERM (Enterprise Relationship Management) - applications managing corporate relations in contacts with the environment (used to search for customer needs and expectations) [22];
- ERP (Enterprise Resources Planning) - a functionally developed category of IT systems containing the MRP II method and enriched with the handling of financial, controlling and human resources[23];
- MIS (Management Information Systems) - Management Information System, are applications supporting enterprise management[24];
- MPS (Master Production Schedule) - main production schedule;
- MRP (Material Requirement Planning) - material needs planning[25];
- MRP II (Manufacturing Resources Planning) - production resource planning[26];

---

16 Słowiński B., *Wstęp do logistyki*, Wydawnictwo Politechniki Koszalińskiej, Koszalin 2008.

17 Kij A. (red.), *Informatyka w logistyce*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2016, p. 47.

18 Ibidem, p. 55.

19 Ibidem, pp. 122-128.

20 Ibidem, p. 59.

21 Majewski J., *Informatyka dla logistyki…* op. cit., p. 51.

22 https://en.wikipedia.org/wiki/Enterprise_relationship_management [Access on: 26.03.20220].

23 Cf. Kij A. (red.), *Informatyka w logistyce…* op. cit., pp. 57-63; Majewski J., *Informatyka dla logistyki…* op. cit., pp. 53-59.

24 https://pl.wikipedia.org/wiki/System_informacyjny_zarządzania [Access on: 26.03.2022].

25 Cf. Kij A. (red.), *Informatyka w logistyce…* op. cit., pp. 53-59; Majewski J., *Informatyka dla logistyki…* op. cit., pp. 85-132.

26 Loc. cit.

- SCM (Supply Chain Management) - a category of IT systems supporting the management of supply chains, supported by: EDI and ADC[27];
- WMS (Warehousing Management Systems) - IT systems used to manage goods stored in a warehouse[28].

2. Another, no less important group of various IT logistics systems are those used in uniformed formations. Taking into account the large number of them, the author, due to his professional experience, focused on displaying examples of logistic systems of the Armed Forces of the Republic of Poland as a hierarchical organization. They include[29]:
   - systems supporting material needs planning;
   - systems supporting the management of the organisation's resources;
   - warehouse management support systems;
   - systems supporting supply chain management;
   - systems for the identification and codification of defense products;
   - LOGIS, SIGMAT, MAG-MAT, SIGMAT-RBM class systems;
   - uniform material index of the Ministry of National Defense - JIM RON;
   - integrated multi-level IT system RON - financial modules (FI - financial accounting, FI-FM - budget accounting, CO - management accounting), FI-AA - fixed assets register, MM / SD - materials management and PM - renovation management;
   - an IT system supporting the management of transport and movement of the AI KONWÓJ troops;
   - "SEW on-line" - IT system supporting personnel resources in the military;
   - LOGFAS - an IT system supporting the planning of logistic support for NATO operations.

Similar and similar, as well as unique solutions in the field of building ICT networks for logistics purposes are currently used in other uniformed formations subordinate to various ministries, with particular emphasis on the Ministry of the Interior and Administration, which supervises the activities of various special services, but also, among others, the Police, Border Guard and the State Fire Service. This naturally results in a multitude of building dedicated information exchange networks tailored to the specifics of a given organization. Of course, they also have the ability to transfer information and data between themselves and the armed

27 Kij A. (red.), *Informatyka w logistyce*… op. cit., p. 47.

28 https://www.streamsoft.pl/system-wms/ [Access on: 26.03.2022].

29 Developed on the basis of: Byłeń S., *Systemy informatyczne wspomagające zarządzanie logistyką w Siłach Zbrojnych Rzeczypospolitej Polskiej*, Wydawnictwo Difin, Warszawa 2020.

forces in accordance with strictly defined rules and procedures. It also proves the heterogeneity of the applied solutions. On the other hand, it should be noted that, as domain networks, they are subject to special supervision and usually they are not allowed to be accessed by unauthorized persons.

The author is convinced that even the best constructed logistic system, regardless of its purpose and type and size of the organization, is prone to disruptions or destruction in circumstances that have not yet been defined in the area of real and potential threats to ICT networks.

4. THREATS TO ITC NETWORKS IN LOGISTICS - AN OUTLINE OF THE PROBLEM

Bearing in mind the considerations so far, it should be emphasized that the nature of threats to IT networks depends on the state and the period of functioning of the state, which includes the time of peace, crisis and war (armed conflict). Each of them causes the logistics area to be more or less affected by the deliberate actions of potential and real adversaries. In the period of peace, it is necessary to address the dangers related to the dependence of logistics ICT networks on the telecommunications infrastructure and, above all, on the global computer network. The most important of them include:

- natural (environmental) hazards that are usually not influenced by humans, such as earthquakes, sinkholes, landslides, lightning, floods and fires;
- anthropogenic threats, related to deliberate (recognition and disruption of radio networks, wiretapping and impersonation of network correspondents, information modification, network intrusion, changes in control, as well as theft) or inadvertent human activity (random accidents, mistakes, accidental loss data).

The above is the foundation for ensuring security for all ICT networks that are not autonomous in the operation of computer networks, but have devices with an Internet connection. In this case, computer incidents of various nature may take place, and the author lists the most undesirable incidents from the point of view of the network user and the organization in Tab. 1:

Tab. 1: Main Threats from the Internet and Their Results

KIND OF THREAT	WHAT LOSSES DO THEY CAUSE?
password-cracking programs	loss of valuable data, private and company documents, access passwords,

keyloggers	stealing passwords and the effects of hard work,
backdoor	access to devices, computer destruction, work monitoring,
phishing	theft of credit card numbers, account passwords,
spyware	they inform those who are interested about the work of the computer user, and provide valuable data
exploit	e.g. they destroy data, steal credit card numbers
viruses and worms	destroy data on disk, data theft
Trojan horses	destroy data on disk, data theft
DoS and DDoS attacks, Flood - overflow	blocking of a computer connected to the network, attempted access by blocking the possibility of processing
unknown programs	cause the operating system to freeze
spam, spamming	clutter your e-mail, this is the sending of unsolicited mail to many recipients at once and the so-called e-mail bombs, the purpose of which is to fill the attacked inbox with, for example, a thousand e-mail messages
internet fraud	steal money
www websites	data capture and analysis when sending forms with confidential data, Java applets, ActiveX, cookies
cracking passwords	most often the so-called dictionary method, via FTP, through the user's account and password, error in scripts, social engineering
computer attack	- collecting information about the system, identifying weak points and attack; - intrusion - entry attempt and seizure of rights; - exiting the system - modification in such a way that it is possible to return
sniffers	by analysing network traffic, they capture packets and passwords, data interception, gradual access to the network,
IP spoofing, spoof, authentication, impersonation	replacement / swapping of the IP address, which results in obtaining unauthorized access to secured networks - The IP is identified as trusted / own
hijacking	intercepting a remote session of a legal user of the system, based on the TCP connection mechanism and generation of the appropriate sequence number.
network address scanning	browsing subsequent IP addresses from the assumed range in order to select a victim or to learn the topology of the attacked network.

scanning network ports: **- sampling**	browsing successive network ports of a computer system in order to obtain information on which ports are open and what services are performed by a given computer system. This is helpful in determining the TCP and UDP services running on the target computer, the type of operating system used by the target computer, specific applications or services provided.
bypassing	bypassing the security process by using an alternative route,
reading	access and familiarization with information to which you are not entitled,
copying	the possibility of copying information by an unauthorized person
stealing	theft of academic achievements, private resources (movies, photos), etc., important data for the company, without leaving a copy in an authorized location
modifying	Unauthorized modification of files, their replacement
deleting	destruction of the attack object

Source: Author's own elaboration

The author made several attempts in his publications to present the most important threats to ICT networks, pointing to their most important aspects. They are important, but at the same time constitute a part of a larger whole, if one takes into account the conditions of logistics operations not only during peace or crisis situations. The period of armed conflict is one of the circumstances least often taken into account by the vast majority of society. The above results from the current lack of threats to the Republic of Poland in the period after the end of World War II. Unfortunately, the current situation on our eastern border has contributed to a broader analysis made by the author in terms of the possibility of the emergence of further threats, which until now were only of interest to the armed forces and other services, guards and inspections included in various uniformed formations. Against this background, the army and its logistics play an extremely important role. In order to fully illustrate the threats to the IT networks of logistics operated by various uniformed services, it should be noted that their basic tasks boil down to the comprehensive supply of their formations with all the necessary and desired means that will allow their undisturbed functioning. In this case, we can say about the need to stock up on weapons, ammunition, fuel and food during a conflict. One should also have the ability to transfer such information through the possessed technical devices and means of communication and IT. ICT networks built and operated for logistics purposes should therefore be protected against the effects of

impact not only on their IT elements, but also those related to telecommunications. The main threats in this area include the following:

- radio-electronic impact on radio networks of own troops, i.e. the possibility of interfering with the operation of radio means in the directions and networks of the KF and VHF bands;
- kinetic (fire) impact on the elements of the developed infrastructure (stationary and mobile / field) dedicated to the needs of defensive operations on the territory of Poland;
- knowledge of threats posed by air attack devices of a potential enemy (airplanes / helicopters);
- the possibility of influencing the developed ICT network by means and equipment of the potential enemy's rocket forces and artillery, taking into account the division into types of armed forces (land forces / navy);
- the possibilities and effects of the impact of weapons of mass destruction (WMD) on ICT networks and their users;
- operation of sabotage and reconnaissance groups of a potential enemy;
- the need to take into account the support of the population for own troops or, worse, national minorities for the soldiers of the potential aggressor and their participation in activities creating situations that may constitute a threat to the own troops' ICT networks;
- the number of stocks and the ability to replenish the losses in the equipment and necessary communication and IT equipment, resulting from the combat operations;
- the possibility of repairing damaged weapons and military equipment as soon as possible.

According to the author, the current international situation has meant that, as this is a significant issue, it can be noticed by following media reports from the region covered by the war in the vicinity of Poland.

When answering the question contained in the main research problem, it should be noted that the security of ICT networks in broadly understood logistics is not permanent. This means that regardless of the situations considered as the state of no immediate threats, it must not be forgotten that the circumstances favourable to the development of logistics may change. Unfortunately, all networks capable of transmitting information become the first target for a determined opponent, regardless of whether he undertakes his actions in virtual or electromagnetic space, or decides to use a force solution to physically destroy it. In this case, you should carefully analyse the potential and actual dangers and try to prevent them using all your forces

and resources. In such a situation, the experience of officers among the commanding staff as well as the implementation and compliance with proven procedures is invaluable. It is logistics and its nervous system in the form of a well-organized information transfer system that today constitute the basis for uninterrupted protection of all goods necessary for various organizations, as well as ordinary citizens.

5. CONCLUSIONS

The author believes that he took up a big challenge trying to outline the general picture of the area being the subject of this study. The analyses carried out allow for the conclusion that the cognitive appetite was awakened and the area of scientific exploration could be shared with several specialists. The volume of the publication and its open nature did not allow for the presentation of many important issues related to logistics ICT networks, as well as organizational and technical details of the currently used solutions. This, however, causes the need for further knowledge and contributed to the continuation of further research. It is also an incentive to start discussions among experts and try to identify solutions that will be necessary to ensure information security, because logistics, regardless of its type and purpose, should respond to the ongoing and comprehensive implementation of all needs and services. It is also worth emphasizing that the awareness of security threats to the ICT network in various organizations is much higher than the common knowledge of citizens on this subject. The same is true of awareness of criminal liability arising from the loss of information. The author's considerations presented above do not exhaust the topic of the study. They are an inspiration for further in-depth research and analysis in this aspect.

This publication is the result of the author's personal reflections. It was assessed that it may be a foundation for further detailed considerations, as the progressive development of technical thought will not be stopped and will also be related to the care for the protection of information provided in logistics ICT networks.

REFERENCES

[1] Byłeń S., *Systemy informatyczne wspomagające zarządzanie logistyką w Siłach Zbrojnych Rzeczypospolitej Polskiej*, Wydawnictwo Difin, Warszawa 2020.

[2] Fierla I. (red.), *Geografia gospodarcza Polski*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2004.

[3] Frączek M., *Zagrożenia i bezpieczeństwo informacji w sieciach teleinformatycznych logistyki*, "Logistyka", (2014)/3, CD 1, pp. 1806-1818.

[4] Frączek M., *Techniczne aspekty bezpieczeństwa systemu łączności w działaniach bojowych na poziomie taktycznym,* "Logistyka", (2014)/5, CD 1, pp. 422-433.

[5] Kij A. (red.), *Informatyka w logistyce*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2016.

[6] Majewski J., *Informatyka dla logistyki*, Instytut Logistyki i Magazynowania, Poznań 2008.

[7] Obarska-Bartmańska M. et al., *Zasady lokalizowania i kształtowania przestrzennego zakładów i zespołów przemysłowych na przykładzie wybranych branż*, Instytut Kształtowania Środowiska, Warszawa 1986.

[8] Rydzkowski W., *Usługi logistyczne*, Instytut Logistyki i Magazynowania, Poznań, 2004.

[9] Słowiński B., *Wstęp do logistyki,* Wydawnictwo Politechniki Koszalińskiej, Koszalin 2008.

[10] Act of 18 July 2002 on the provision of electronic services, OJ 2002, no. 144, item 1204.

[11] Winiarski B. (red.), *Polityka gospodarcza,* Wydawnictwo Naukowe PWN, Warszawa 2004.

[12] Witkowski K., *Zarządzanie infrastrukturą logistyczną gminy,* [in:] *Wybrane zagadnienia logistyki stosowanej*, Wydawnictwo Polskiej Akademii Nauk, Kraków 2005.

[13] https://sites.google.com/site/historialogistyki/home/etymologia-logistyki

[14] https://pl.wikipedia.org/wiki/Logistyka

[15] https://www.logistyka.net.pl/slownik-logistyczny/szczegoly/4,adc

[16] https://pl.wikipedia.org/wiki/B2B

[17] https://www.logistyka.net.pl/slownik-logistyczny/szczegoly/44,b2c

[18] https://www.karierawfinansach.pl/baza-wiedzy/slownik-pojec/b2c-co-to-znaczy-b2c

[19] https://www.system-kanban.pl/definicja/bom-bill-of-materials

[20] https://broneks.net/wp-content/uploads/2017/09/ebok-wprowadzenie-do-logistyki-bslowinski.Pdf

[21] https://en.wikipedia.org/wiki/Enterprise_relationship_management

[22] https://pl.wikipedia.org/wiki/System_informacyjny_zarządzania

[23] https://www.streamsoft.pl/system-wms

Mariusz Frączek
Pomeranian University in Słupsk, Poland
mariusz.fraczek@apsl.edu.pl
ORCID: 0000-0002-2216-8053