

Systemy Logistyczne Wojsk
Zeszyt 60 (2024)
ISSN 1508-5430, s. 165-180
DOI:

Instytut Logistyki
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

Military Logistics Systems
Volume 60 (2024)
ISSN 1508-5430, pp. 165-180
DOI:

Institute of Logistics
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

Internet of things as a tool for ensuring material security of Military Units and Institutions

Internet rzeczy jako narzędzie zapewnienia bezpieczeństwa materiałowego jednostek i instytucji wojskowych

Mieczysław Pawlisiak

mieczyslaw.pawlisiak@wat.edu.pl; ORCID: 0000-0003-2501-8779
Military University of Technology, Faculty of Security, Logistics and Management, Poland

Oleh Maslii

mon2369@ukr.net; ORCID: 0000-0003-2809-2763
Deputy Head of the Academy for Academic Work, Odesa Military Academy

Abstract. Material security of military units and institutions is one of the determinants of the ability to carry out combat tasks. It will be possible to provide it, among other Things, by obtaining information on the existing material needs and the possibility of meeting them. This information can be obtained through the use of technologically advanced technologies such as the IoT. The aim of the article is to present the results of research on the impact of the IoT, logistical security of military units and institutions. In order to achieve this goal, a general research problem has been identified in the form of a question: "How will the IoT affect the acquisition of information necessary to make decisions regarding the satisfaction of the material needs of military units and institutions"? The solution to the general research problem was achieved by refining it with four specific research problems. Theoretical methods (analysis, synthesis) supplemented by an empirical method – participant observation – were used to solve them. An important item in the research process were the results of surveys conducted with persons performing tasks related to ensuring material security in military units and institutions. The results obtained in the course of the research clearly indicate the importance of information for decision-making related to meeting the material needs of military units and institutions. On the other hand, the ability to provide material resources will depend not only on the resources at hand, but mainly on the time of obtaining information on the occurrence of needs in a specific place and time. This requirement can be met through the use of modern technologies such as the IoT. In addition to the undoubted benefits, the results of the study also pointed to the possibility of threats during the use of the IoT. Therefore, it is necessary to balance the benefits and threats and make a decision on the possibility of implementing the IoT for solutions supporting the implementation

of material security tasks for military units and institutions. The content of the article indicates that the assumed goal has been achieved by indicating the importance of the IoT for the implementation of tasks related to meeting the material needs of military units and institutions.

Keywords: security, material security, military unit, IoT, information

Abstrakt. Bezpieczeństwo materialne jednostek i instytucji wojskowych jest jednym z istotnych determinantów zdolności do realizacji zadań bojowych. Możliwe będzie jej zapewnienie m.in. poprzez uzyskanie informacji o istniejących potrzebach materialnych i możliwości ich zaspokojenia. Informacje te można uzyskać dzięki wykorzystaniu zaawansowanych technologicznie technologii, takich jak Internet Rzeczy. Celem artykułu jest publikacja wyników badań wskazujących, czy i w jakim stopniu Internet Rzeczy będzie determinował bezpieczeństwo logistyczne jednostek i instytucji wojskowych. Chcąc osiągnąć ten cel, zdefiniowano ogólny problem badawczy w postaci pytania: „w jaki sposób Internet Rzeczy wpłynie na proces decyzyjny dotyczący realizacji zadań z zakresu bezpieczeństwa materialnego w jednostkach i instytucjach wojskowych, a tym samym będzie decydował o ich bezpieczeństwie materialnym?”. Rozwiązanie ogólnego problemu badawczego uzyskano dzięki rozpatrzeniu trzech szczegółowych problemów badawczych. Do ich rozwiązania wykorzystano metody teoretyczne (analiza, synteza) uzupełnione metodą empiryczną – obserwacją uczestniczącą. Istotną pozycję w procesie badawczym stanowiły wyniki badań ankietowych przeprowadzonych z osobami wykonującymi zadania związane z zapewnieniem bezpieczeństwa materialnego w jednostkach i instytucjach wojskowych. Wyniki uzyskane w trakcie badań jednoznacznie wskazują na znaczenie zaspokojenia potrzeb materialnych dla zapewnienia bezpieczeństwa jednostek i instytucji wojskowych. Oprócz niewątpliwych korzyści, wyniki badania wskazały również na możliwość wystąpienia zagrożeń podczas korzystania z Internetu Rzeczy. W związku z tym konieczne jest wyważenie korzyści i zagrożeń oraz podjęcie decyzji o możliwości wdrożenia Internetu Rzeczy dla rozwiązań wspierających realizację zadań bezpieczeństwa materialnego dla jednostek i instytucji wojskowych.

Słowa kluczowe: bezpieczeństwo, bezpieczeństwo materialne, informacja jednostka wojskowa, Internet Rzeczy

Introduction

Material security of military units and institutions is possible after meeting two key conditions. They concern the possession of adequate executive capacity and information allowing for rational exploitation of that capacity. The executive capacity is always adequate to the organizational level at which it occurs, while the information is necessary to decide on how to use the components of this potential. (Saaty, 2008, pp. 112 - 123). Therefore, it can be assumed that information is the component that is the prime requirement, the fulfillment of which gives the opportunity to decide how to ensure material safety for military units and institutions. It is also important to understand the importance of the time of obtaining the information necessary to make decisions. Involving only a human being for this purpose, one should consider a situation in which delays may occur and thus the reaction in the form of a decision may be delayed. Therefore, it is necessary to look for solutions that allow to minimize or even eliminate these risks threatening the time of obtaining information. Such an opportunity is provided, among others, by the IoT as a modern tool allowing for the exchange of information in real time (Miller 2016, pp. 21 - 32). This is a challenge that should be considered, and a detailed analysis should be made in terms of the possibility of implementing the IoT and using its

capabilities to support decision-making processes to ensure the material security of military units and institutions in the 21st century. In view of the above justifications, the *area of research* is the Internet of Things and its impact on the logistical security of military units and institutions. Adopting such an assumption, it is justified to state that the main research problem is to answer the question “*How the IoT will affect the acquisition of information necessary to make decisions regarding the material needs of military units and institutions?*” Such a broadly formulated research problem requires clarification by specifying detailed research problems, which, according to the author, include:

1. How should the concept of material security of military units and institutions be understood in the 21st century?
2. What is the importance of information, and especially the time of its acquisition, for ensuring material security?
3. What modern technological solutions can be used to obtain information in real time regarding the state of material security of military units and institutions?
4. What opportunities and threats to the material security of military units and institutions are generated using the IoT in the process of obtaining information necessary to make decisions regarding the use of the executive capacity of material services?

Considering the adopted area of research, it was assumed that *the purpose of the research* will be to indicate whether and to what extent the IoT will determine the logistical security of military units and institutions. At the same time, on the basis of information obtained during the analysis of theoretical studies and professional experience gained during military service in positions in the logistics division of the Armed Forces of the Republic of Poland, it is justified to adopt the *hypothesis* that the IoT as a source of information will be an important factor allowing for timely decision-making. Thus, it may contribute to ensuring the material security of military units and institutions.

The solution to the general research problem and specific research problems resulting from it requires the use of appropriate research methods and tools. The *theoretical methods*, namely analysis and synthesis, are primarily useful and give the possibility of obtaining correct results. However, they will be supplemented by the *empirical method* – participatory observation used by the author in the real-time satisfaction of material needs in military units and institutions as well as while training activities – exercises conducted on qualification courses at the Military University of Technology. An extremely helpful *research technique* was conducting surveys with people performing tasks related to meeting material needs in military units and institutions. A total of 89 people were involved. The participants perform military service in various official positions being the executor of material security tasks or the recipient for whom logistical security tasks are carried out. Such a

diversity of positions of people subjected to surveys gives the opportunity to view issues related to logistics security from different points of view and thus the reliability of the results is at a high level.

The results obtained during the research will allow for the recommendation of solutions the use of which in the real activity of material services may constitute an important contribution to ensuring material security of military units and institutions in the 21st century.

The essence of material security of military units and institutions

The term “*security*” in the 21st century is inflected by many cases. It is also sometimes interpreted in any way. However, this depends on the understanding of the entity to which it relates, as well as the subject of what security is for a specific entity. One can find the statement that safety is nothing more than a state giving a sense of certainty and a guarantee of its preservation and a chance for improvement (Pawłowski, Zdrodowski, Kuliczkowski ed. 2020, pp. 28 - 34). Such an approach defines the concept of security in a broad way and is universal because it can apply to every area of human activity. Another view is presented by W. Kitler (2020, pp. 44 - 52), who in his study is of the opinion that security concerns people (individuals, social groups, organizations), but only where people function there is a need for security understood as the pursuit of a life free from interference to conditions of existence and development. It can be considered that such a position clarifies the concept of security by addressing it directly to the human being. Yet another but extremely interesting claim is that the idealistic approach to defining the concept of security means that it is a state of humanity without threats. Realism obliges to discern the possible threats that are imminent, and security should refer to the possibility of counteracting them in the event of their occurrence (Rutkowski 2018, pp. 19 - 20). One can also find the statement that safety as a state should be perceived as a category considered in theoretical and synthetic (practical) terms. As subjective security, it applies to all individual and collective entities (Ficoń 2018, p. 10).

The cited views and statements of various authors dealing with security issues indicate the absolute need to perceive security as such through the prism of the subject and object. In other words, first of all, you need to answer the question of who this security concerns. Knowing the answer to such a question, one can put a second one regarding what constitutes the basis for the subject to have a sense or conditions that allow its existence and development. In conclusion, it can be taken for granted that whenever dealing with security as such, it is first necessary to define what (who) the actor is and what this actor needs or expects in order for his/her security to be ensured.

Considering the essence of material security of military units and institutions, there are no problems with defining the entity to which this security applies. These are military units and institutions with an appropriate organizational structure filled with personnel – people and military equipment necessary to perform the tasks assigned to them. The answer to the question of what the subject of material safety is somewhat more complicated. Well, in the Armed Forces of the Republic of Poland there are five classes of material services according to which tasks related to meeting material needs are carried out. These include:

- (a) Class I - supplies for consumption by both personnel and animals, occurring in uniform rations irrespective of local combat or field conditions;
- (b) class II – means of supply, including medicinal products and medical devices, for which tables of amounts receivable or equipment have been established;
- (c) Class III – fuels, oils and lubricants for all uses, excluding aviation;
- (d) Class IIIA – aviation fuels, oils and lubricants used in aviation;
- (e) class IV – means of supply, including structural and fortification materials, for which tables of amounts receivable or equipment have not been established;
- (f) Class V – combat resources. (Logistics Doctrine of the Armed Forces of the Republic of Poland D-4 /B/, version 2, pp. 105 - 106).

The classification of supplies presented above indicates the broad spectrum of needs that can be considered as the material security component of an entity such as military units and institutions. However, it is important to take a broader look at the scope of material needs. It is not only the product specification that plays a role in ensuring material safety. It is necessary to further clarify what this material safety consists of. Additional elements (parameters) determining the material safety of military units and institutions should be indicated here. According to the author, it is crucial to indicate at least four determinants. All of them play a key role in ensuring material safety, and the order in which they are presented does not indicate their hierarchical location. Therefore, the importance of an appropriate supply range to ensure logistical security should be indicated first. As a message, it should be indicated that the assortment delivered to the recipient must be identical to the reported or generated needs. In practice, this means providing means of supply corresponding in the first place to the types of military equipment operated. For example, tank ammunition must go to the armored units and not to the sub-units of the mechanized troops. The second determinant of material safety is the appropriate time, understood as an obligatory term ensuring the continuity of ownership of each of the means of supply. Minor time delays may be allowed, especially in Class IV, as this assortment is not a means of primary need. However, the timely delivery of combat resources, propellants and lubricants is crucial. Without these means of supply, it is difficult to fire on the enemy and there is no possibility of maneuvering

and moving, which in conditions of war is an absolute necessity in the 21st century. As a confirmation of this thesis, we can quote the words of the Chief of Staff of the US Army, Gen. Mark Milley, who once said, "If you stay on the battlefield for more than two or three hours, you will be dead." (Freedberg, Sydney, 2016). This content is an impulse to consider how to organize the delivery of supplies to ensure material safety for military units and institutions, considering the appropriate assortment and time of delivery. According to the author, it seems necessary to emphasize at least two other determinants. This applies to quantities, as in different conditions of functioning or the implementation of combat sentences, the needs in terms of quantities will not be the same. Therefore, an adequate amount is necessary to enable military units and institutions to carry out the tasks assigned to them. The place of supply is also important as a complement to the previously mentioned factors. Therefore, meeting the requirement to fulfill the content of four key requirements, it can be assumed that material safety will be ensured and from this point of view there will be positive conditions for the correct implementation of tasks by military units and institutions.

Information in the process of meeting the material needs of military units and institutions

Information in the general sense should be understood as a set of specific data that, in relation to meeting material needs in military units and institutions, constitute the basis for starting the decision-making process related to the use of a specific potential of the material subsystem (Griffin, 2017, pp. 26 - 44). This means that information constitutes and will constitute in the future a starting point for undertaking specific activities in the process of satisfying material needs generated in military units and institutions. It is important to determine the requirements that this information should meet to ensure material safety. Based on the tests carried out, it is considered that the essential requirements for material protection concern four areas. In the first place, the respondents believed that the information should be useful for people to whom it is addressed, i.e. those who are responsible for the implementation of tasks related to meeting material needs in military units and institutions. With this in mind, it is justified to make the right selection due to which the relevant information is only sent to those people who need it to fulfill their job responsibilities. The second requirement indicated by the respondents concerns the deadline for providing or obtaining information. It should be recognized that the subjects decided that the information should be up-to-date and communicated to the addressee at a time when it could be equally useful. It can also be considered that a possible delay in a certain sense may disqualify its usefulness in the process of performing tasks related to meeting material needs and thus ensuring material

safety of military units and institutions. The data obtained in the survey process shows that the source of information is important for its recipient (Sikorski, 2020, pp. 21 – 23). Implicitly, it can be assumed that this source is to be verified, thanks to which the information obtained can be considered reliable and objective, containing a description of the actual and current state of the situation in the material subsystem. The last requirement to which the respondents turned their attention concerns the completeness of information. It is important for the recipient of the information that it does not include any gaps or ambiguities, as guesses or assumptions may lead to a situation in which the actions taken do not ensure the material safety of the protected unit or military institution.

With a specific set of information, it seems necessary to realize that it is not only characterized by complexity, large amount of data and dynamics of the number of changes that can occur in the management process. It is also important to have a properly configured organizational structure filled with people who are qualified to use this information appropriately. In addition to the appropriate qualifications, these people should, and in principle must, be equipped with the right instrumentation, which is not a high-end computer, but at the same time the appropriate software installed on them. Such a human – device – software symbiosis gives reason to believe that the information will enable material potential to be managed and thus ensure the material security of military units and institutions (Ścibiorek, Borucka, 2022, pp. 147 – 160).

The general indications of the importance of information in the management process for meeting the material needs need further clarification. It should therefore be pointed out that the first activity in this area is the collection of information. It is the activity of obtaining, which is sometimes referred to as procurement. To carry out the related activities, it is necessary to have, after prior preparation, an appropriate system, the elements of which are usually full-time organizational units occurring in the material division at various organizational levels of the Polish Armed Forces. These may sometimes be an ad hoc organized element, such as reconnaissance groups, which, because of their activities, may acquire information on, for example, infrastructure useful for material security tasks. The essential sources of information necessary for taking actions to ensure material safety are, in the first instance, the subordinates, who in periodic or ad hoc reports include all issues related to the material security status of the level to which the report relates (LOGFAS fundamentals and basic data operator course tutorial, ed. NATO Communications and Information Agency, Brussels 2019, pp. 12 - 125). Another source of information may be the supervisor, who can inform the subordinate how he will provide material support using his own resources. Practice indicates that particular attention should be paid to the information already held by the person or people responsible for carrying out the material security tasks. After all, it is knowledge, skills, experience, and the

knowledge base built by professionals from material services that can provide added value in the area of information collecting in material services.

Recording information on the material subsystem is an important activity. It involves documenting material information in one place in such a way that it can be used by different people. This can be done 'manually' by handwriting or graphically presenting specific information about the material subsystem. This method is most prevalent at lower levels of command which is due to the relatively small amount of information and the lack of physical capability to use electronic devices (computers). Recording may take place in a slightly different way at higher organizational levels (operational level), in which case there may be the use of information systems for recording data and depicting material situations in military units and institutions.

Due to the amount of information, it is important to select it. It can be conducted using various criteria that are usually set by the supervisor. Based on the conducted research, it appears that the substantive content is the most important, and it determines what and when it should be communicated to other participants in the process of meeting material needs, and on this basis, it should reach the right audience. In practice, this means that, for example, information on the functioning of the combat service goes to the person responsible for supplying ammunition to subordinate divisions. In the practice of material security tasks, detailed criteria for verification and selection of information can also be found. These may include:

- a/ important, key, essential, unimportant, irrelevant,
- b) certain or requiring additional confirmation or verification,
- c/ complete or incomplete requiring supplementation,
- d/ communicated electronically or in writing.

Handling of information also includes its recording. Observing technological progress, the task involved appears to be easy to complete. In the 21st century, the tasks involved seem to be easy to perform. It is possible to record in a traditional way through the physical collection of written or graphic documents. This method is widely used at lower organizational levels – subdivision. On the other hand, higher organizational levels, e.g. a troop, a tactical unit, where the amount of information is definitely higher, technological achievements are used using appropriate devices where folders containing material information are created from files and digitized documents, which can be used in the future to organize material security of military units and institutions.

An important activity in dealing with information is its classification. It consists in assigning specific content to predetermined levels, e.g. confidentiality or access levels. This consists in deciding which information must be treated as strictly secret, secret, confidential, or proprietary (Journal of Laws 2019.0.742 Act on the protection of classified information. The legal status is valid as of: 03.03.2023. Chapter 3). The formal requirement is that the level of secrecy is always decided by the person who is the decision maker at the considered organizational level, e.g. the head of S-4

decides on the classification in the brigade. Another method of classification may refer to the organizational levels appearing in the structures of the Armed Forces of the Republic of Poland. Therefore, information may be used and related to the implementation of material protection tasks at the first or second tactical level as well as assigned to the operational level.

One of the final actions concerning the information on the activity of the material subsystem is its distribution. It consists in making certain content available through established channels of information to persons for whom this information is necessary to fulfill their duties in their official position. Activities related to this may take place through personal contact or transmission of certain content using, among others, electronic systems. Specific solutions regarding the transmission of information at individual organizational levels are included in the normative documents known in the Polish Armed Forces as "Standard Operating Procedures." They apply at all levels of organizational military logistics. One of the key findings of these procedures is the indication of compliance with the rules on the protection of classified information. This allows to discover to whom and what information related to the operation of the material subsystem can be transmitted.

The final stage in the process of dealing with information regarding the satisfaction of material needs and thus ensuring material security is its storage (archiving). The general arrangements for the related activities are set out in the provisions on where, when, for what period, and who is obliged to store certain information. They may also have internal arrangements adopted at a certain organizational level, but these arrangements may not contradict the ministerial arrangements. The physical form of archived information may take the form of a so-called "paper" document or an electronic medium of information.

Proper handling of information on the operation of the material subsystem in accordance with the procedures in force in this respect may be a guarantee of the correct implementation of tasks, which will translate into ensuring the material security of military units and institutions. The results of the conducted research indicate that the basis for ensuring material security is firstly the obtainment of information, and then its distribution after prior selection and appropriate classification. They are therefore an indication of how to organize the acquisition and distribution of appropriately selected information on the functioning of the material subsystem. This will allow for satisfying the generated material needs and thus ensure their material security.

Modern technologies in the process of obtaining information on the state of material security of military units and institutions

As previously justified, it is necessary to have up-to-date information in order to make an accurate and timely decision. This requirement results, i.e., in the development of new electronic technologies, and in particular of various ICT devices. It is in every activity of a person performing military service in the material subsystem that information and knowledge have become the key to the correct implementation of material security tasks and thus ensuring the material security of military units and institutions. It is noted, however, that there is a certain regularity in the fact that people with longer service experience and thus more advanced age present more conservative views in this area. This is because they do not believe in the benefits of using, for example, the IoT and believe that it is enough to use traditional means of communication – radio stations and documents in physical form. The results of the research also indicate that young people are convinced to use modern technological solutions, which allows them to obtain the same information in a much shorter time. This, in turn, allows not only for timely decision making, but at the same time gives the opportunity to correctly perform the task of satisfying the generated material needs.

Such a situation, according to the author, is a sufficient premise to present the way (idea) of the functioning of the IoT. First, it is necessary to clarify what the Internet of Things is and what it is about. The IoT is a digital network that connects various physical objects, which may be elements of the equipment of the Polish Armed Forces. The contact between individual elements of the system is multi-vector, which results in the fact that communication takes place not only in the relation between a specific object and one addressee. In real time, the same information reaches all devices logged into a specific digital network. This can be described as a kind of web in which everyone communicates with everyone in real time (Miller, 2016, pp. 33 - 62).

In order to ensure material security, as previously explained, it is necessary to provide the right recipient at the right time such quantity and range of supplies that allow to perform the assigned tasks. So how to use the achievements related to the implementation of the IoT in this process. This can be presented on the example of a situation that may take place in current training activities as well as in the course of the implementation of tasks on a possible future battlefield. The assumed starting point is the wear of the shells for the KRAB cannon-howitzer. Each projectile is equipped with a microscopic sensor, which, after firing the projectile – in real time (immediately), places information about this event on the network or sends it to the indicated recipients. These recipients are devices located in different places. First of all, this information can be used by the commander knowing that the number of usable missiles has decreased. The same information is sent to the person managing

the material security and their documents record the current state of ammunition for the KRAB cannon-howitzer. At the same time, the weapons storekeeper is informed about the need to provide the missing ammunition, which should be prepared for transfer to the means of transport. It may also be the case that such information is obtained by the operator of the means of transport that are necessary to deliver the missing ammunition (Banerji, Kumar, Mittal, Chaubey, 2023). An extensive digital network can inform not only military authorities entering the scales of the material subsystem about the situation. A signal can also be sent to the manufacturer of ammunition with an existing need, which is an impulse to undertake the production of a specific type of combat means.

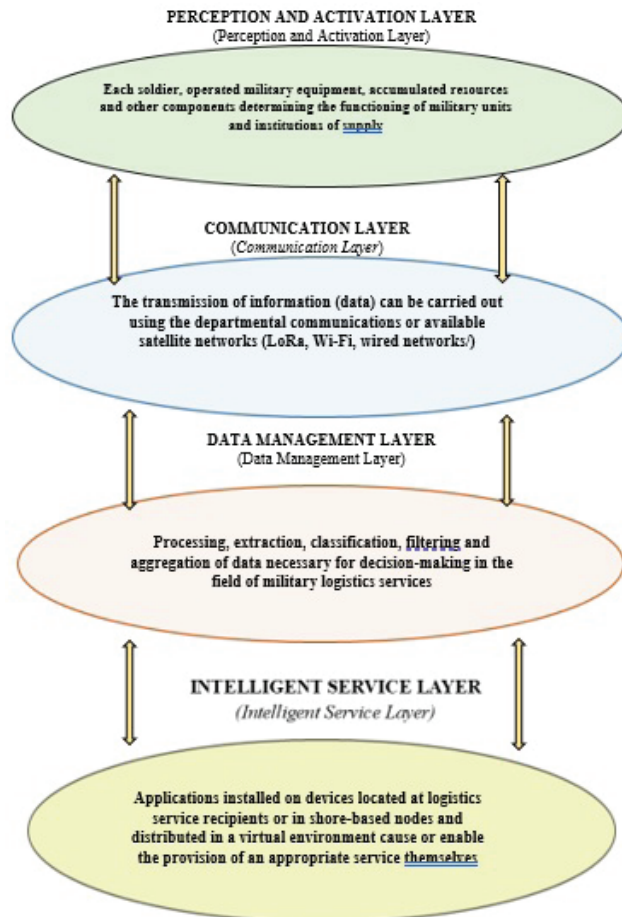


Fig.1. The structure and functioning of the IoT in the material substrates

Source: <https://www.wojsko-polskie.pl/wat/articles/najlepsze-publicacje-4/2021-03-25c-ieee-communications-magazine-o-internecie-rzeczy-w-zastosowaniach-wojskowych/> [10. 04. 2023].

The presented idea of using the IoT to ensure material security in relation to a single supply measure can also be presented in the form of the following scheme. It was developed on the basis of the content contained in the online article located at <https://www.wojsko-polskie.pl/wat/articles/najlepsze-publicacje-4/2021-03-25-ieee-communications-magazine-o-internecie-rzeczy-w-zastosowaniach-wojskowych/> [10. 04. 2023].

When analyzing the content and at the same time detailed solutions accompanying the process of implementing the IoT solutions in the material subsystem of the Polish Armed Forces, it should be noted that this is undoubtedly a great challenge. However, according to the author, action should be taken comprehensively. This means that not only material safety should be taken care of, but when implementing the IoT, all components of the logistics system can be covered by this solution. This will then contribute to ensuring a comprehensive exchange of information in the logistics system, which may contribute to ensuring the logistical security of military units and institutions.

The IoT in the material subsystem – opportunities and threats

The implementation of modern technological solutions such as the IoT in the process of ensuring material security of military units and institutions is not a solution that should be perceived only in terms of positives. It also results in the need to face various challenges, which does not preclude the desire to use technological progress to ensure material safety for military units and institutions. Many interesting and informative observations result from the content of the answers contained in the surveys. Due to the size of the research sample (89 people were surveyed), the obtained results should be considered correct and have not only cognitive but also scientific value.

The design of the question and the possible content of the answers regarding the benefits of using the IoT in the material subsystem allowed respondents to choose the two most important answers in their opinion. Nearly 70% of the responses indicated that the most important benefit is the time of obtaining information. However, the indications of other benefits did not turn out to be unambiguous, as none of them exceeded the figure of 11%. This means that the persons surveyed consider that the benefit of access to information of those persons who are interested in the material situation and its completeness are equally important. The lower value for the respondents is certainty as to the content of the information provided and the possibility of identifying the source from which the specific information comes. The results obtained can be interpreted as partly an objective state, because the participants of the survey are professional soldiers and, at least to a limited extent,

should understand the importance of the functioning of the material subsystem and its impact on the material safety of military units and institutions.

The content presented above is the result of an analysis of the answers obtained during the survey. When generalizing the content contained in the studies on the use of the Internet of Things in the functioning of broadly understood logistics, it is possible and even necessary to pay attention to issues other than those mentioned (Oborski, 2015, pp. 52- 71). Therefore, using the IoT, the possibility of continuous inventory monitoring can be considered positive. From the point of view of material security of military units and institutions, this is a significant positive, because it gives the possibility of current management of owned resources and at the same time may affect their rational use both during the current functioning and in conditions of threat or war. Another benefit may be to reduce a person's effort by replacing it with devices for transmitting, collecting, archiving and processing information. Somehow, an additional benefit may be to avoid mistakes or mistakes that a person can make. The unquestionable benefit of using the Internet of Things is the ability to aggregate and select information. This is particularly important in relation to the resources of the material services of the Polish Army due to the fact that the number of material items, taking into account, for example, the shelf life, is very large. It is even several million positions.

When presenting the benefits of using the IoT in the real operation of material services, one should not only see the benefits, but also the threats that this system may generate. An interesting approach is the view that the IoT itself is not a threat, but that the first threat may be a human (Atzori, Iera, Morabito, 2010). It is a man with his weaknesses, character imperfections or lack of appropriate knowledge that may be the weakest link in the use of a modern tool which is the IoT.

The content of question number 9 in the surveys concerned possible threats resulting from the use of the IoT in the process of meeting the material needs of military institutions. Most respondents identified the human being as a component of the entire system, which may generate the greatest threat. It is hard to disagree with such views. It is enough to observe that today's reality, in which a human, using the achievements of technology, makes various mistakes, which result, among others, in personal data theft, which consequently leads to financial, material and image losses (Krawiec, 2020, pp. 47 – 68). It can therefore be envisaged that also a human operating the software used by the IoT for the material subsystem of the Polish Armed Forces may be the weakest link generating various threats. As important from the point of view of material security, the respondents considered the possibility of intercepting information by the adversary and the possibility of disinformation. These are two important aspects because the opponent, knowing the state of the material resources and the location, can try and make strikes to destroy the accumulated supply. Such activity can currently be observed in Ukraine, where its armed forces, using the available means of destruction, effectively destroy supply of

especially fuel and ammunition. Another no less important threat is the acquisition of information by the adversary and its use for misinformation. It is not difficult to imagine a situation in which food transport is supplied to a military unit with an ammunition shortage and the unit waiting for fuel supplies receives ammunition. This can lead to chaos and loss of the ability to perform specific tasks. Therefore, it is important to counteract possible threats in advance, the consequences of which can sometimes be even tragic. Projects are already underway that can at least limit the possible threats in the future.

The results obtained during the survey indicate that the first step to using the IoT safely is to ensure it is operated by a professional - a man who will ensure that all the standards set for information security are followed. Subsequently, the respondents indicated the need to use only the original, usually autonomous software. In practice it should be software dedicated to a specific, single system, e.g. the logistics system of the Polish Armed Forces. Being aware of the difficulties in applying such an autonomous solution, other standard software can be allowed, bearing in mind the need to update it on an ongoing basis, which is the basis for its safe use. It is the software update that allows you to eliminate possible gaps that can be used by a potential opponent to disrupt the functioning of the IoT. The responses of the respondents also indicated the need for additional safeguards in the form of the use of multi-stage safeguards consisting in at least two-stage verification. Other responses suggested the use of unique passwords and encrypted access codes. There were also voices suggesting a reduction in the number of people using the IoT, but it seems that the Standard Operating Procedures precisely define the activities of functional people in the material subsystem. Their number is always adequate to the number and quality of problems that these people solve. While pointing out the possibility of reducing threats and thus ensuring the safe operation of the Internet of Things in the material subsystem, all components must be taken care of on an ongoing basis and react in a timely manner to possible irregularities. Only such a procedure can provide the opportunity to correctly exploit the benefit of the IoT to ensure material security of military units and institutions.

Conclusions and recommendations

Material security of military units and institutions is the basis for their performance in peacetime training as well as in the conditions of threat and war. This forces a number of organizational and executive actions to be taken to supply the recipient with the right quantity, quality, to the appointed place and at the right time. The implementation of these projects is always preceded by decision-making activities, which are the domain of management bodies at every organizational level of the Polish Armed Forces. It is the decision that forms the basis for undertaking

real physical activities related to the satisfaction of material needs in military units and institutions. In the first place, during the current – peaceful implementation of tasks, the accumulation and appropriate distribution of inventories of supplies takes place. These activities, due to peaceful conditions, do not pose challenges addressed to the material subsystem. The importance of material security is beginning to be appreciated by individuals and military institutions especially during times of danger and war. Then the dynamics of operations take place and the changes that occur require having the information necessary to make decisions on how to ensure material security for military units and institutions. Then, the use of the IoT may be a solution that will meet the basic requirements for making the right decisions in time to deliver supplies and thus provide material security for military units and institutions. It is the Internet of Things that in real time is able to provide complete and reliable information without which it would be impossible to make decisions related to the implementation of material security tasks. An important recommendation resulting from the conducted research is to indicate the need to implement solutions regarding the IoT in the process of tracking the consumption of artillery and tank ammunition. Such reasoning of the respondents is justified because the ammunition of larger calibers is easier to equip with appropriate electronic devices and, moreover, this type of ammunition can determine success on the modern battlefield. Therefore, the use of the IoT in the material subsystem of the Polish Armed Forces may contribute to ensuring the material security of military units and institutions, especially in conditions of threat and war.

BIBLIOGRAPHY

- [1] Atzori L., Iera A., Morabito G., 2010, The Internet of Things: A survey, „Computer Networks”, 54.
- [2] Banerji G., Kumar Y., Mittal Y., Chaubey M., 2023. A Study on Internet of Military Things a. 4 IITM Journal of Information Technology, 9, 28 – 35.
- [3] Ficoń K., 2020. Bezpieczeństwo narodowe i jego typologie, Warszawa, BEL Studio.
- [4] Freedberg Jr., Sydney J., Miserable, Disobedient & Victorious: Gen. Milley's Future US Soldier. [Online] Breaking Defense (blog), October 5, 2016, Available at: <https://www.jstor.org/stable/pdf/resrep19583.8.pdf> [Accessed: 2 April 2023].
- [5] Griffin R., 2017, Fundamentals of Organization Management, wyd. PWN Warszawa, 2017.
- [6] IEEE Communications Magazine o Internecie Rzeczy w zastosowaniach wojskowych [online], Available at: <https://www.wojsko-polskie.pl/wat/articles/najlepsze-publicacje-4/2021-03-25c-ieee-communications-magazine-o-internecie-rzeczy-w-zastosowaniach-wojskowych/> [Accessed: 10 April 2023].
- [7] Journal Of Laws 2019.0.742 Act on the protection of classified information. The legal status is valid as of: 03.03.2023. Chapter 3.
- [8] Kitler W., 2018, National Security Organization of the republic of Poland. Systemic, legal, administrative and systems aspects, wyd. A. Marszałek, Toruń.
- [9] Krawiec J., 2020 Internet of Things. Cybersecurity Issues, wyd. Oficyna Wydawnicza Politechniki Warszawskiej.

- [10] Logistics Doctrine of the Armed Forces of the Republic of Poland D-4 /B/, version 2, Bydgoszcz 2019, 105 – 106.
- [11] LOGFAS fundamentals and basic data operator course tutorial, wyd. NATO Communications and Information Agency, Bruksela 2019,
- [12] Miller M., 2016, Internet of Things, PWN Warszawa,
- [13] Oborski, P., 2015, Integrated monitoring system of production processes. Management and Production Engineering Review.
- [14] Pawłowski J., Zdrodowski B., Kuliczkowski M. (ed.), 2020, Glossary of security terms, A. Marszałek, Toruń,
- [15] Pisz, I., Sęk, T. i Zielecki, W., 2013. Logistics in the company, PWE Warszawa,
- [16] Rutkowski C., 2018, Fundamentals of security sciences with elements of science, SGSP Warszawa,
- [17] Saaty, T. L., 2008, Decision making with the analytic hierarchy process. International Journal of Services Sciences, 1 (1).
- [18] Sikorski J., 2020, Internet of Things, PWN Warszawa.
- [19] Ścibiorek Z., Borucka A. 2022, Information in the decision-making process, Military Logistics Systems, 56(1).