

BUSINESS CONTINUITY MANAGEMENT OF LOGISTICAL PROCESSES IN THE STATE SECURITY AND DEFENCE SYSTEM

Tomasz JAŁOWIEC^{1*}, Ewa DĘBICKA²

¹ War Studies University, Management and Command Faculty, Warszawa; t.jalowiec@akademia.mil.pl

² Motor Transport Institute, Warszawa; ewa.debicka@its.waw.pl

* Correspondence author

Abstract: In the light of research conducted both in Poland and scientific centres abroad, it should be noted that one of the concepts that are becoming more and more popular in the state security and defence sector is the concept of business continuity management. With regard to logistical processes, it is used in a special way to ensure their smooth running through the proper preparation of logistical entities to continue operations at a previously accepted by the client level in the event of disturbances.

In the light of the above, the aim of the article is to identify the possibility of common use of the assumptions of the concept of business continuity management in the process of managing logistical processes within the state security and defence system.

Keywords: management, continuity, logistics processes, security, defence.

ZARZĄDZANIE CIĄGŁOŚCIĄ DZIAŁANIA PROCESÓW LOGISTYCZNYCH W SYSTEMIE BEZPIECZEŃSTWA I OBRONNOŚCI PAŃSTWA

Streszczenie: W świetle badań prowadzonych zarówno w Polsce jak i w zagranicznych ośrodkach naukowych, należy zauważyć, że jedną z koncepcji cieszących się coraz większą popularnością w sektorze bezpieczeństwa i obronności państwa jest koncepcja zarządzania ciągłością działania. W odniesieniu do procesów logistycznych jest ona wykorzystywana w sposób szczególny do zapewnienia ich niezakłóconego przebiegu poprzez właściwe przygotowanie podmiotów logistycznych do kontynuowania działań na akceptowalnym przez klienta, wcześniej określonym poziomie w sytuacji wystąpienia zakłóceń.

W świetle powyższego za cel artykułu przyjęto identyfikację możliwości powszechnego wykorzystania założeń koncepcji zarządzania ciągłością działania w procesie zarządzania procesami logistycznymi w systemie bezpieczeństwa i obronności państwa.

Słowa kluczowe: zarządzanie, ciągłość działania, procesy logistyczne, bezpieczeństwo, obronność.

1. Introduction

The occurrence of disturbing factors is a natural element of the functioning of the state security and defence systems. They have different origins and their effects affect all phenomena and processes occurring in the sphere of state defence and security. In the light of the negative impacts, a key issue in many cases turns out to be taking actions aimed at ensuring business continuity as a prerequisite for the correct implementation of a wide range of tasks in these two key areas for every country. It is worth emphasizing that among the processes carried out by the elements of the above-mentioned systems, the priority role is given to logistical processes, which through the cyclical supply of material resources determine the undisturbed operation of entities responsible for security and defence of the state. Moreover, in accordance with expectations, the transfer of necessary goods and their proper storage form the basis for the current functioning of many entities in the field of state security and defence. In the light of research conducted both in Poland and the scientific centres abroad, it should be noted that one of the concepts gaining popularity in the state security and defence sector is the concept of business continuity management (BCM). Its use is focused primarily on the identification of threats and continuous introduction of appropriate safeguards to manage or eliminate them. With regard to the logistical processes, it is used in a special way to ensure their continuity of action through proper preparation of logistical entities to continue operations at the customer pre-defined level in the event of disturbances occurring.

In the light of the above, the aim of the article is to identify the possibility of widespread use of the BCM concept in the process of managing logistical processes in the state security and defence system. The research problem to be solved was formulated in the form of a question: what and to what extent determines the use of the BCM concept in the process of managing logistical processes in the state security and defence system? As a result of the research conducted, conclusions and postulates were formulated, which may form the basis for further research on a problem extremely important from the perspective of the state security and defence.

2. The essence and scope of business continuity management concept

The origins of the concept of business continuity management date back to the late 1960s in the United States of America, when considering the widespread use of information technology, plans for emergency IT systems began to be developed. Over time, business continuity management found many supporters among the management team of key business processes. So in the 1980s and 1990s, business continuity management was necessary in the

face of natural disasters and the wave of terrorist attacks. As a consequence, this led to the development of normative documents of the ISO 22000 series, thematically assigned to the business continuity. The ISO 22301: 2012 standard, *Societal security – Business continuity management systems – Requirements* is the result of international cooperation and the compromise reached. The standard defines the requirements related to planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continuous improvement of a documented management system, which aims to protect against any situation that may lead to disruption, loss, emergency or crisis. In addition, it improves the ability to prepare for such situations, responding appropriately when they occur, and returning to normal functioning if they occur. These requirements are of general character and intended for use in all organizations regardless of the type, size or nature of the activity. Business continuity management is a holistic management process that identifies potential threats and the effects these threats may exert on the organization's activities in the event of their occurrence, which provides framework structures for building resilience of the organization and enables an effective response to protect the interests of its key stakeholders, its reputation, brand and value-creating activities. It is therefore a natural response to the needs of entities responsible for security and defence of the state, which in a conscious way want to manage threats and minimize their effects. The list of certificates issued in 2014 prepared by ISO (International Organization for Standardization), among the others, testifies to the fact that this standard is gaining more and more popularity. In total, 1757 certificates for compliance with the requirements of the ISO 22301 standard were issued in 2014. An unquestioned leader is India with the total of 480 certificates, which constitutes almost 30% of the total number of the certificates issued. Next is the United Kingdom – 345 certificates and Japan – 200 certificates. Last year, 20 implementations in Poland ended with certification.

The events that may threaten business continuity can be divided into two groups:

- events that occur suddenly – e.g. violent fire, explosion, traffic accident, terrorist attack, etc.; plans associated with such events must therefore take into account the surprise factor;
- changes in the operating environment that cause a gradual increase in the risk – e.g. flood, prolonged power failure, etc.; in this case, it is possible to take actions early enough to prevent some of the consequences of these events, or at least try to minimize them.

The essence of ensuring business continuity is, first and foremost, appropriately preparing the organization to continue operations at the level accepted earlier by the client in the event of disturbances. In the state security and defence system these will be both quantitative and qualitative requirements (e.g.: timely performance of the service, number of operations performed, security of entrusted property and entrusted data). To this end, the following activities must be carried out:

- define the internal and external context of the company's operation, which will help to identify areas of potential threats,
- analyze the business impact, i.e. assess the impact of disruptions in business conducted, determine and select the business continuity strategy, as well as identification of processes for which business continuity plans should be developed,
- carry out a risk assessment process consisting of risk identification, analysis and evaluation,
- establish business continuity plans, i.e. a set of documented procedures that prepare the organization for the appropriate response, resumption and restoration of functioning to the pre-determined level after the occurrence of the disruption.

BCM is a process by which the organization prepares for future incidents or crisis situations that could jeopardize the organization's basic mission and its short- and long-term ability to stay operational and meet the expectations of the stakeholders. CM, considered the main element of BCM, is about how the organization should inform the public, its employees, business partners and stakeholders about the disaster or crisis situation and the steps taken to restore business operations and minimize the impact on internal and external stakeholders. The main elements of BCM are:

1. **Management support** – the management provides support to properly prepare, maintain and execute a business continuity plan (BCP) by allocating adequate resources, people and financial means.
2. **Risk estimation and mitigation** – potential risks arising from threats such as fire or flood are determined, as well as their probability and potential impact on the organization. This is done on-site at branch level to ensure that the risks associated with all possible events are understandable and properly managed.
3. **BIA (business impact analysis)** – identifies processes that are an integral part of maintaining the organization's operations in the event of a disaster and determines how quickly integral processes should be resumed after its occurrence.
4. **Resumption of business and continuity strategy** – indicates concrete steps, people and resources needed to resume essential business processes. It also identifies key mechanisms and information protocols. The strategy may include patterns and standards of a given company or sector.
5. **Knowledge of the plan and training** – training in business continuity plans and knowledge about it are necessary to manage business continuity. The training may also consist of performing exercises and/or examining practical issues regarding fragments of the business continuity plan.
6. **Maintenance, service, servicing** – the BCM's ability and documentation are maintained so that they remain effective and consistent with the organization's priorities.

Due to the general nature of the requirements of the normative document, the possibility of implementing them among entities responsible for security and defence of the state is large.

It seems that in order to ensure the proper functioning of the aforementioned key areas for each country, ensuring business continuity at the level of each implemented process is indispensable. All the more so in the face of new threats (embargo, legal changes, increasing anxiety in the European countries, cybercrime) one should consciously and comprehensively prepare for their possible consequences so that the processes are not interrupted. The basic benefits of business continuity management are, among the others:

- minimizing costs related to the disruption of the ongoing processes,
- gaining a competitive advantage,
- increase of trust among clients and business partners,
- meeting legal, normative and business requirements to ensure the continuity of the processes carried out,
- conscious decision making,
- strengthening the organization's resistance to threats,
- monitoring and early identification of new threats,
- rational and adequate selection of solutions for resuming and restoring the functionality of processes to a fixed level.

In conclusion, it should be pointed out that the essence of business continuity management is the comprehensive preparation of the organization in the event of the occurrences that may pose a threat to the proper functioning of individual elements of a given system. Examples of such events may be: fire, flood, terrorist attack or armed conflict, but also a long-term failure of the power system or telecommunications channels. Due to the nature of the tasks carried out by the entities responsible for the security and defence of the state, taking cyclical actions to eliminate or limit the effects of the abovementioned phenomena turns out to be crucial in many cases.

3. Using the assumptions of the business continuity management concept in the process of managing logistical processes in the state security and defence system – empirical research

In order to solve the research problem defined in the introduction, apart from theoretical studies, empirical research proved necessary. For this purpose, the method of a diagnostic survey conducted using the expert interview method was used. The research, conducted from September to November 2017, included seven experts representing theoretical and practical dimension of the state's security and defence system. All the experts had many years (from 19 to 27 years) experience in the implementation of logistical processes in the sphere of security and defence of the state, as well as in terms of ensuring their continuity of operation. Due to the limited nature of the conducted research, the research tool developed (the questionnaire sheet)

contained only one question referring directly to the research problem posed. It was – *What and to what extent determines the widespread use of the BCM concept in the process of managing logistical processes in the state security and defence system?*

At the beginning of the research, in view of the multitude of definitions of logistical processes present in the literature, the logistical process is defined as one in which the distribution, condition and flows of its components, i.e. people, material goods, information and financial resources, requires coordination with other processes due to the criteria of location, time, cost and effectiveness of meeting the organization's desired goals. The key logistical processes include: basic processes, e.g. forwarding, transport, warehousing, packing and assembling the loads; loading processes: loading up, unloading and offloading; auxiliary processes, e.g. repair and renovation processes, designing the order fulfilment, labelling, offering logistical services; information processes, e.g. documenting and monitoring of activities and processes; service processes, also called "management" processes, e.g. forecasting and planning activities, negotiating and concluding contracts, setting priorities and financing activities.

As a result of the research it was possible to obtain the research material containing expert opinions on the determinants of the general use of the BCM concept assumptions in the process of managing logistical processes in the state security and defence system. A detailed analysis of expert statements indicates that the positions presented by them can be divided into three basic groups. The first of them indicated that when considering the state security and defence system in terms of the possibility of using the concept of business continuity in the management of logistical processes, such determinants could be:

1. **Information** – "... information used in the management of logistical processes of the security and defence system should bear hallmarks, of authenticity, non-repudiation and reliability, legibility and processing capacity. If any of these factors are missing, an event occurs, which results in disturbing the continuity of the management process. Loss of both integrity, reliability or the ability to process information, as well as access to it results in a temporary disruption of the continuity of the logistical subsystem functioning in the security and defence system ...".
2. **Reliability** (timeliness, quality and size) and organization of deliveries – "... one of the elements of the defence and defence system is the defence industry. The lack of implemented business continuity concept may cause problems in the implementation of production processes, maintaining product safety (e.g. inadequate quality of production materials), etc".
3. **Maintaining the strategic reserves at the appropriate level** – "... their lack may cause that the logistical subsystem will not be able to guarantee conditions for e.g. counteracting emerging internal and external threats in the functioning of the state's security and defence system ...".

4. **Reliability of the organizational structures** responsible for the implementation of logistical processes – "... especially in the event of threats or instability of the system – duplication of competences, operational scenarios, etc ...".

Among the experts there also dominated opinions that the main determinants in the process of managing logistical processes related to ensuring business continuity in the state's security and defence systems include the following:

- protection of an appropriate, interference-resistant communication system of all authorities involved in ensuring continuity of supplies,
- ensuring real-time tracking and monitoring of stocks necessary for the functioning of the state in crisis situations,
- securing unimpeded fuel supplies for units in a state of full combat readiness,
- ensuring ongoing tracking and monitoring of supplies for the security and defence of the state,
- war inventory management process of material and combat resources, their optimal distribution at the following levels: strategic, operational and tactical,
- cooperation of defence industry entities with the relevant organs and central institutions of the Ministry of National Defence in the field of obtaining military equipment and production of the above-mentioned means.

The third group of presented views focused on indicating that the factor conditioning the widespread use of the BCM concept in the process of managing logistical processes in the state security and defence system is, above all, the time that determines many activities. Experts pointed out that "... especially if we are talking about a security and defence system, it is the time that influences the decisions made, the model of the decision making structure, etc. There are many elements in the security and defence system that it will influence. For example, crisis management. A crisis response plan is probably nothing more than a certain scenario of action at the moment the threat occurs. Also there is there logistics and logistical processes management (transport and evacuation, accommodation, medical care). Additionally, in crisis situations, the adopted organizational structure determines the response time (a decision making). It should be as flattest as possible. There is also a critical infrastructure. Here this is asking for the business continuity plans to be created. Maintaining it properly determines the capabilities of the state security and defence system ...".

Trying to synthetically summarize the results of empirical research, it should be emphasized that all experts in their statements pointed to the main goal to be assumed in the ongoing work aimed at widespread use of the concept of business continuity in the management of logistical processes in the state security and defence system. In their opinion, it should refer to ensuring resilience and the ability to effectively respond to a wide range of threats to protect the key interests of the state. Such an objective will determine and somehow direct the work aimed at guaranteeing the conditions for the proper conduct of logistical processes, on which depends

the implementation at the required level of tasks set by the entities responsible for the security and defence of the state. In the light of the collected research material, it should be noted that the problem raised for consideration turned out to be extremely complex and multifaceted; therefore, it seems justified in many respects to conduct further, extended research on this phenomenon, which is extremely important for the state security and defence system.

4. Summary

The results obtained in the research process authorize the author to make the following general **conclusions**, i.e.:

1. Logistics processes in the state security and defence system are exposed to a number of threats.
2. Despite the occurrence of many threats, the use of the concepts of business continuity management is currently not a common phenomenon in relation to the management of logistical processes in the state security and defence system.
3. In the current conditions of the state functioning there are real needs and premises for the universal implementation of the assumptions of the concept of business continuity management in the management of logistical processes in the state security and defence system.
4. Reliable information, reliability, maintaining the strategic reserves at the right level, reliability of organizational structures, time, adequate interference-resistant communication system and real-time tracking and monitoring are the main determinants of the continuity of logistical processes in the state's security and defence system.
5. The widespread use of business continuity assumptions in the management of logistical processes in the state security and defence system, due to their specificity, will require working out and implementing formal procedures, both at the central level and individual entities responsible for state security and defence.

The material outlines only selected aspects regarding the use of the concept of business continuity in relation to the management of logistical processes in the state security and defence system. The adopted restrictions allowed achieving the assumed goal, while indicating the directions of further research. In conclusion, it is worth pointing to the real need to continue scientific research aimed at solving the problems outlined in the material. Such activities may contribute to the improvement of the functioning of logistical processes implemented in the said systems, and thus ensure the proper functioning of entities responsible for security and defence of the state, which, without the cyclical supply of material goods, are unable to carry out the tasks set before them.

Bibliography

1. Dębicka, E., Jałowiec, T. (2015). Zarządzanie ciągłością działania we współczesnej logistyce. *Gospodarka Materialowa i Logistyka*, 5.
2. <http://barbaszewski.pl/Dydaktyka/ISO27k-rozd11.pdf>.
3. <http://docplayer.pl/7771520-Zarzadzanie-ciagloscia-dzialania.html>.
4. Krawczyk, S. (2001). *Zarządzanie procesami logistycznymi*. Warszawa: PWE.
5. Łunarski, J. (2009). *Zarządzanie jakością w logistyce*. Rzeszów: Politechnika Rzeszowska.
6. Norma PN-EN ISO 22301:2014-11. *Bezpieczeństwo powszechne. System zarządzania ciągłością działania. Wymagania*.
7. *The ISO Survey of Management System Standard Certifications -2014. Executive summary*, www.iso.org.