Scientific Journal of the Military University of Land Forces
ISSN: 2544-7122 (print), 2545-0719 (online)
2022, Volume 54, Number 2(204), Pages 245-255
DOI: 10.5604/01.3001.0015.8976

Original article

The role of information in crisis management

Zenon Zamiar, Zbigniew Ścibiorek*

Faculty of Logistics and Transport,
The International University of Logistics and Transport in Wrocław, Poland,
e-mail: z.zamiar@msl.com.pl; zbscibi@wp.pl

INFORMATION

Article history:

Submited: 14 December 2020

Accepted: 17 August 2021

Published: 15 June 2022

ABSTRACT

The article emphasises that current conditions for monitoring and ensuring homeland security are increasingly complex. The complexity of many processes and their difficult conditions emphasise the need to make relatively quick decisions. Following this requirement, much more attention is being paid to improving the functioning of information systems. It was emphasised that the increasing amount of information is, on the one hand, a positive phenomenon, but on the other hand it is not always conducive to making a reasonably quick decision. It is necessary to strive to obtain, through various channels (methods), reliable information, which will be the basis for making decisions, dismissing security threats and (or) minimising their effects. It was emphasised that the path to achieving the objectives is different in each case; no universal methodology can be presented. In addition to the conditions, a number of proposals aimed at improving the activities of those in leadership roles and the functioning of crisis management teams are presented.

KEYWORDS

security, homeland security, crisis management, information

* Corresponding author

Introduction

The current security situation is not beneficial to society and individuals, and even to the environment. A number of factors contribute to this assessment. Globalisation and the accompanying process of internationalisation of all activities have an impact on what is happening with regard to internal security. The growing impact of the pandemic situation is also of great importance. Increasingly, the environment is forcing the need to modify one's behavior and respond rationally to the variability of the environment [1, p. 315].

Contemporary conditions force a number of changes in the strategy of internal security management and crisis management. It is no longer enough to just follow some proven rules that have been effective in the past. The rule stating that certain decisions cause certain effects, and the most often predictable ones, is not enough today. Today, the relationship between the cause and effect of a decision is more complex. Decision-makers are required to think long-term when acting, and to think and act ahead. The phenomenon of the uncertainty of tomorrow plays an important role. All these phenomena make flexibility of action a permanent part of the strategy, and not only in relation to crisis management. In such a situation, the art of security management must evolve to meet the requirements of the changing environment – the conditions [2, p. 600-661] of our functioning. We have reason to believe that the future is a compilation of diverse phenomena and processes that will be impossible to reduce to a common denominator. Nowadays, it is necessary to adopt a specific, often international perspective of examining a number of phenomena related to crisis management. It is also important to remember that there is no one universal style in crisis management. Qualifications, theoretical and practical knowledge of management methods and techniques in a diverse environment are needed. Creativity and diplomatic and negotiating skills are not insignificant.

Globalisation, pandemics, and accompanying phenomena have imposed incredibly difficult conditions for homeland security [3, p. 12]. In many cases, these conditions require constant adaptation, sometimes even revolutionary, to the increasingly changing and more complex environment.

Achieving a satisfactory state of internal security depends mainly on the use of the consequences of technological changes related to telecommunications, *software and hardware*, enabling the acceleration and mastering of information processing and the creation of systems such as the Internet and other information banks [4]. Decision-makers must be future-oriented individuals, embodying self-reliance, creative thinking, independence and willingness to take risks, as well as able to acquire and manage the information held.

The aim of the article is to show the role of information in crisis management, while the issues under consideration were not related to a specific situation or the environment – the place where a crisis occurred. The publication sought to address the research problem of how and when information is used in crisis management. A working hypothesis was adopted assuming that the efficient flow of information between authorities and structures responsible for crisis management is primarily to prevent crisis situations, and in cases when they occur, to remove their effects effectively. The verification of the adopted hypothesis was preceded by a pilot study (research reconnaissance). The main research was a diagnostic survey of 132 respondents whose professional activity is directly and (or) indirectly related to security issues at various levels of local government.

1. Safety is an overriding category

Since ancient times, man has been trying to subdue the natural environment, introducing changes in it to make life easier and more comfortable. A man tries to make himself independent of the unfriendly forces of nature. Civilisation reduces the number and destructive power of natural threats, but it also generates new types of threats. It means that a human being lives and will live in an environment of potential security threats which, when activated as a result of unfavorable changes in natural or civilisation space (a particular stimulus), may turn into a particular type of real threats – events unfavorable to life or health, or to the environment.

There is an opportunity to shape the level of security. Its condition is not a stable condition – it is not a good given to the subject once and for all. There are constant security threats in the real world from both natural forces and the unintended and intended effects of human activity. In each case, the security system of a given entity should be adapted to its potential threats and the desired level of security. For this purpose, it is necessary to develop the entity's security management procedures and to optimise its information and decision-making processes.

Managing internal security, and thus reacting to crisis situations, is one of the basic functions of all public authorities and administration, both at the governmental and local levels. This is mainly due to the fact that security is seen as one of the basic values and needs of the security subject, which include, among others: certainty of existence and survival, guarantee of development, undisturbed possibility of possession, identity, political independence or improvement of the quality of life of society. Despite a certain universality, the above set of values and needs is not a fixed set and is related to the security entity within a defined scope and in time space. This set requires protection against real or potential threats, which are characterised by unpredictability, suddenness, multidimensionality, volatility, indeterminacy and interpenetration, and affect almost all areas of society. However, the changing conditions of the security environment require the improvement of the internal security system and adaptation to contemporary threats and challenges. In addition, some threats to internal security, such as terrorism, international organised crime and cross-border migration, are international in nature or, such as disease epidemics, epizooties or radiation contamination, do not stop at national borders. Therefore, consistently combating them or counteracting their effects requires cooperation between states or international organisations. This "set" should be supplemented with what can be the source of crisis situations, which are defined as "situations that adversely affect the level of safety of people, property to a large extent or the environment, causing significant restrictions in the operation of competent public administration bodies due to the inadequacy of the forces and means held" [5, Art. 3(1)]. They may be caused by such phenomena as: natural disasters, technical and construction failures, traffic accidents, hazards with chemical and petroleum derivatives, epidemiological and epizoological threats, public order disturbances or acts of terrorism. Emergencies are unexpected, sudden phenomena that destabilise the safety of the population. Therefore, it is necessary to prepare and organise activities in advance in order to be able to react as quickly as possible in the event of an incident. To counter such a wide range of security threats, information is indispensable.

2. Information as a basis for decision-making

No one needs to be convinced that information is the basis for decisions. When it comes to emergencies, each event (phenomenon) is different. This in turn means that, in general, information can be used for one case that is usually unique. In practice, we often base our choices on too small a sample of information, leading to poorer verdicts. On the other hand, it turns out that information substitutes make it much easier to choose between two options, thereby reducing the cost of exploration.

Interdisciplinary knowledge is essential for effective decision making. Experience also plays a big role. However, it cannot be an essential consideration in evaluating the events and information to be considered in making a decision. Making decisions always requires talent and special skills supported by appropriate qualifications. They are not something permanent. Nowadays, the need for constant improvement of competences is natural. Nowadays, it cannot be forgotten that functioning in an increasingly dynamic environment generates newer types of risks, which should also be identified in a continuous and systematic manner.

Regardless of the circumstances, the activity of individuals responsible for internal security is to anticipate problems, find their causes, find solutions and take actions necessary to implement them. This process is most effective when it is carried out in a systematic way, without "shortcuts and madness", although analysing the "historical decisions", it is hard to resist the impression that the more crazy, risky – the better. Ingenuity and intuition play a fundamental role both in the search for solutions and in the key moments of making decisions [6, p. 11].

The decision-making process begins when such information reaches the decision-maker, which makes him aware of an objectively existing decision-making situation and triggers his readiness to act. Based on this, a decision problem is formulated for which finding a solution prompts the decision maker to actively search for alternatives. The starting point is to diagnose the problem, that is, to determine where the problem lies. Therefore, a lot also depends on the information competence of the person. Information competences should be understood as the ability to search and use information, as well as the ability to obtain information in an effective manner, while at the same time being able to critically and competently select, evaluate, synthesise and use it in a creative way, according to specific needs, with the conscious use of an appropriate strategy for finding this information. A person with information competences must be able to determine their own information needs, locate the necessary information, evaluate it and use it effectively [7, p. 81].

The knowledge of crisis situations allows to determine the information needs for workplaces or organisational units of the appropriate element of the security management system, and at the same time adequate to the level of its location in the higher-level structure. The extent of these needs depends on the level of management (leadership). This is understandable, because the decision-making cycle is a specific type and sequence of activities involving the processing of input information into a specific output information, which is the decision.

The list of information needs can be developed in two variants: in terms of the communication source or in terms of the receiver. In the first case, the set of information needs is drawn up according to the organisational units or workplaces where the sources of information are located and from where the necessary information is sent to the appropriate addressees. In the second solution, lists of information needs are developed for workplaces where specific decisions are to be made.

In any situation, the information system [8, p. 18] provides an understanding of the existing situation as well as a forecast of its development. It is understandable because the right decision, which determines the achievement of the assumed goals, depends on the properties of the information held. In turn, this means that a well-organised information system should meet certain conditions. First of all, it must be adapted to the needs and cover all areas of activity of a given opinion-making and advisory body or management team (center). In addition, it must provide comprehensive and up-to-date messages, as well as provide information to those who need them in a form suitable for direct use (without processing) and most convenient for decision making. It is no less important that the information system ensures the efficient use of the news through the speed and frequency of its circulation; this means that the information should be up-to-date, complete, and properly sorted. Such requirements for the considered system result primarily from the fact that the information influences the final shape of the decision. However, there are doubts about how to separate true from false information.

The ease of human access to information is accompanied by an excess of information and the resulting difficulties. In a flurry of information, it is very easy to miss the most relevant ones. Information overload is one of the most acute effects of the development of modern information and communication technologies. The phenomenon of *information overload* is a natural consequence of the increasing supply of information. The costs of their distribution are systematically decreasing, but the possibilities of information processing by humans have not increased significantly over the last few decades. In the professional literature, it is also referred to as: information overload, information explosion, information bomb, information overproduction, information flood, information deluge or information smog meaning a suffocating excess of worthless or even toxic information. Information overload is hardly a new phenomenon [7, p. 74-75; 9, p. 101].

Nowadays, it is difficult to disagree with D. Sumper, that we are *surrounded by numbers*, that technological development, and people's dependence on computers and the Internet is constantly increasing [10]. Today, regardless of how information is defined, it has always been an important factor in the progress of civilisation. People seek to expand their knowledge by gathering information, publishing it, and exchanging it with others, and the development of computer networks facilitates this exchange on a scale previously unimagined.

Constant acquisition of necessary information and its use is one of the basic tasks of persons and institutions responsible for security. Practice shows that the broader and richer the range of information held, the easier it is to control the actual day-to-day needs and opportunities of management in risk-generating situations thus individuals can shape their future and their relations with the environment in a more confident way. The right information and the right flow of information have a major impact on the behaviour and conduct of people, it is the art of mobilising and stimulating the energy and intelligence of all those contributing to tasks, and it influences management processes. They make it possible to capture the changes taking place, to formulate appropriate assumptions and to select the most likely future actions.

Such great importance of information results not only from the fact that it constitutes the basis for a decision – to solve a decision problem. One way to protect any organisation is to secure its information space. Whoever controls the information space controls a range of phenomena, not excluding crisis situations. This axiom is as old as humanity. Today, information is a real powerhouse. At the same time, we must not become slaves to an excess of information [11, p. 341].

The struggle for reliable information, obtained at the right time, is one of the priorities of activities not only of managers. It is no exaggeration to say that without current and complete information, the decision maker is "blind" [12, p. 49-66]. The above-mentioned paradigm of business activity management applies to crisis management in its entirety.

When discussing the issues of information, one cannot ignore the issues that are commonly referred to as information overload and the resulting information chaos. In the context of the issues raised, it is important to manage information. J. Szczupaczyński believes that modern IT systems can solve information management problems [13, p. 21-22]. However, there is an abundance of evidence to show that this is not the case. In addition to highly efficient devices, it is always necessary to recognise a human being; after all, he is the consumer of information [14, p. 83]. It should also be remembered that new technologies allow access to more information, but this probably increases the risk of various types of mistakes [15, p. 231]. They cannot be afforded in crisis management.

3. We live in a world of information

Nowadays, the constantly developing technology has an increasing impact on the life and functioning of the world, country and man. Alvin Toffler rightly points out that in the information society, the winner is the one who has access to information and who has the skills to process it in everyday life. Currently, information is one of the most important values of civilisation, and thanks to the availability of the Internet, which is the source of widely understood information, we have access to it almost at any time. We can use a wide range of information, remembering to properly segregate it, because on the one hand the Internet is a powerful source of knowledge, but on the other hand it also contains a lot of false information. The problem of modern society lies in skillfully separating these two aspects from each other and learning to do it effectively.

The information collected should only be used to enhance security. The Internet as a communication tool and the whole sphere of information technology is the fastest developing element of modern social life. It is not only an unstoppable area of activity and development, but also a very difficult place to control (in the positive sense of the word), for the purpose of preventing all symptoms and phenomena of crime and assaults on human and social existence [16, p. 109]. Nowadays, the ICT network is the nerve network of the country, and the undisturbed operation of cyberspace is the basis of the undisturbed functioning of the economy, but also the security of any country [17, p. 43].

In the era of universal access to various types of electronic media, unlimited possibilities of information exchange between participants of social, economic and political life, the question arises whether this environment itself is not a threat to its users? Every day we convince ourselves of the useful sides of the use of cyberspace in general, in which we carry out our daily life functions, social, cultural, etc., but on the other hand we get disturbing information about the dark side of the development of ICT techniques. Threats in cyberspace, such as cyber surveillance, cyber crime, cyber terrorism, or cyber warfare, keep ICT systems and critical infrastructure protection professionals awake at night and challenge governments whose responsibility it is to ensure the security of the state and its citizens.

Nowadays we cannot imagine doing any business without the Internet and various types of IT networks. It is not only the possibility to exchange various information indispensable for making decisions, e.g. investment, allocation or related to monitoring and ensuring safety.

4. Online safety should also be remembered about

The universal use of the Internet and the increasing importance of the availability of services offered by the Internet make it necessary to sensitise citizens to the problem of ICT security, and thus raise their awareness of safe methods of using the Internet. Each user of a computer and other sources of information should remember that the use of the global network, in addition to its benefits, also entails a number of threats, even if they are unnoticeable to them. That is why it is so important to spread awareness among the entire society of the dangers in the global network and the need to counteract cyber threats. Awareness and knowledge of how to prevent and combat threats are key elements in combating them. Only responsible user behaviour can effectively minimise the risk arising from existing threats. It should be emphasised that in the modern world, ensuring ICT security does not depend only on the activities of specialised government institutions and ICT security specialists. With the spread of Internet access at home, the change in the way computer attacks are carried out, and users increasingly seen to be ignorant or careless, the responsibility for security falls on every computer user. This is the time when pedagogy, and especially media education, should pay attention to the dangers of cyber-terrorism.

According to P. Neumann and D. Parker, harmful activities in cyberspace can be divided into [18, p. 181], among others:

– viewing and stealing information,

– data falsification,

– destruction of information,

– impersonating someone else,

– intentional mismanagement of the system,

– using other systems to create malicious programs.

The *National Security Strategy of the Republic of Poland*, in the chapter on new security challenges, points to the growing importance of new, unusual threats, the source of which are also becoming difficult to identify non-state entities. It emphasises the tensions and instabilities caused by international terrorism, proliferation of weapons of mass destruction, and the unpredictable to the end policies of authoritarian governments. By exposing the so-called holistic approach, it does not identify specific reasons for the emergence and development of political terrorism in Poland. First of all, it refers to international institutions and their functional capabilities.

The network security is very important from a crisis management perspective. If there is no secure IT system, it is difficult to expect reasonably quick and rational security decisions.

5. Research and the results

The research was conducted in the third quarter of 2020 in Lower Silesia. For the purpose of quantitative research, a purposeful sample selection was adopted based on the selection of research subjects from the population of people whose professional activity is related to issues directly and (or) indirectly related to security issues, especially internal security and crisis management, as well as postgraduate students, mainly in the field of *Internal Security and Crisis Management*. As part of the sample, N = 132 respondents with higher education were selected, including – 28% (37 respondents) directly related to crisis management. Nearly 85% – 112 respondents declared that homeland security issues were in their area of professional interest. For the purpose of the study, the N sample was divided into four categories:

– police officers – n_1 = 32 (24%),
– municipal police officers – n_2 = 43 (33%),
– individuals who are part of crisis management teams – n_3 = 37 (28%),
– postgraduate students – n_4 = 20 (15%).

It should be noted that of all 37 respondents who are part of crisis management teams, almost 80% (30 respondents) have completed postgraduate studies and specialised training in homeland security or crisis management.

The quantitative research used the method of diagnostic survey conducted with the technique of survey research using an electronic survey questionnaire. They were intended to identify opportunities for obtaining reasonably reliable information and the acceptability of its use in solving complex homeland security problems.

The questions in the survey were open ended, conjunctive – single choice or disjunctive – multiple choice based on a cafeteria of response options. The purpose of the survey was to obtain answers to questions focused on the following problems:

– the importance of information in crisis management,
– the premises of the "fight" for information,
– forms of improvement of methods directed at effective use of obtained and/or acquired information.

A summary of the study results is included in Table 1. Their analysis is the premise for a number of conclusions. Regarding the issue of verifying information, regardless of its source, the vast majority of respondents see such a necessity. Nearly 77% of respondents favor such a solution. Two facts are worth highlighting. First of all, only half of the Police officers, 56% to

Table 1. Summary of test results

Question	Police officers – 32 officers		Municipal police officers – 43 persons		CM team members – 37 persons		Postgraduate students – 20 persons	
Do you follow the rule on the need to verify information?	Yes	No	Yes	No	Yes	No	Yes	No
	18 (56%)	14 (44%)	32 (74%)	11 (26%)	30 (81%)	3 (17%)	19 (95%)	1 (5%)
Who should be the primary source of information:								
– superior level	11 (34%)		18 (42%)		19 (52%)		8 (40%)	
– subordinates	14 (44%)		12 (28%)		12 (32%)		9 (45%)	
– other sources	7 (22%)		13 (30%)		6 (16%)		3 (15%)	
At what time should information from a supervisor at the Poviat Crisis Management Team level be used:								
– immediately after acquisition and evaluation	3 (9%)		5 (12%)		2 (6%)		1 (5%)	
– up to 30 minutes	16 (50%)		21 (49%)		26 (70%)		17 (85%)	
– up to 1 hour	13 (41%)		17 (39%)		9 (24%)		2 (10%)	
At what time should information from a supervisor at the Municipal Crisis Management Team level be used:								
– immediately after acquisition and evaluation	3 (10%)		5 (12%)		13 (35%)		0	
– up to 10 minutes	18 (56%)		31 (72%)		21 (57%)		17 (85%)	
– up to 30 minutes	11 (34%)		7 (16%)		3 (8%)		3 (15%)	
When should the available information be used at the level of:								
– WZZK [Provincial Crisis Management Team]	up to 60’	up to 120’	up to 60’	up to 120’	up to 60’	up to 120’	up to 60’	up to 120’
	8 (25%)	24 (75%)	12 (28%)	31 (72%)	19 (51%)	18 (49%)	16 (80%)	6 (20%)
– PZZK [Poviat Crisis Management Team]	up to 30’	up to 60’	up to 30’	up to 60’	up to 30’	up to 60’	up to 30’	up to 60’
	13 (41%)	19 (59%)	13 (30%)	30 (70%)	23 (62%)	14 (38%)	18 (90%)	2 (10%)
– Municipal Crisis Management Team	up to 15’	up to 30’	up to 15’	up to 30’	up to 15’	up to 30’	up to 15’	up to 30’
	15 (47%)	17 (53%)	16 (37%)	27 (63%)	29 (78%)	8 (22%)	19 (95%)	1 (5%)

Source: Own study based on empirical research.

be exact, perceive such a need. Second of all, there is a belief among postgraduate students about the validity of checking the information that is available for use.

The assessment of the question: *who should be the main source of information*, is quite varied. The predominant belief is that it is the superior level's responsibility to provide information to its subordinates (42% of the total surveyed). These are the findings, but they are thought-provoking. Conclusions from many exercises unequivocally prove that in crisis management, assessment of phenomena unfavorable to security, the most important are opinions or reports of those who are at the scene of the event (phenomenon). It is true, however, that the supervisor generally has a much broader (larger) perspective of the perception and context of the conclusions, especially with respect to the forecast, but those who see it, convey a reasonably realistic picture. This position was also presented by slightly over 37% of the respondents who believed that the subordinates were the primary source of information.

The next two questions referred to the issue of when information obtained from a supervisor should be used. The respondents predominantly represented the poviat and municipal levels of government, and therefore the survey focused on these levels. The predominant belief in both cases was that the information held should first be evaluated and then used. At the same time, the members of the municipal crisis management teams were of the opinion that time plays an important role in responding to unfavorable events. Therefore, they were in favour of using the information as quickly as possible – up to 10 minutes (92% of respondents). A similar judgment prevailed at the poviat level, where 76% of respondents believed the information obtained from the superior should be used within no more than half an hour.

The issue of using the information held, but without identifying its source, was addressed in the next questions. In this case, the respondents' positions provoke reflection and are not convergent with regard to representatives of individual groups. With respect to the provincial level (WZZK), the vast majority was of the opinion that there is a need for adequate time to assess the information held. At the same time, the members of the crisis management teams were divided in their opinions. Half of them (51%) indicated time up to one hour, and slightly longer time up to two hours was indicated by 49% of the respondents. "Haste" was prevalent among students, where 80% were in favour of using the information in no more than one hour.

With respect to the poviat level, divergent views prevailed regarding the use of the information held. Poviat Crisis Management Team employees and students were of the opinion that the information held should be used in a fairly short time – up to 30 minutes (76% of both groups). The predominant belief was that when in possession of information regarding a defined event (phenomenon) threatening safety, one should, within one hour, use his knowledge.

At the municipal level, there was also no consensus on the timing of the use of the information held. The staff of the CM teams felt that it was important to respond as quickly as possible. This meant that 78% of people were of the opinion that the time was perceived to be up to one quarter of an hour. Students were also in favor of quick action (95%). Their position on time was unchanged. In terms of time use across all the questions, they tended to respond relatively quickly to what the information provided. Such a position probably resulted from the fascination with modern ICT solutions, which could be felt during backstage conversations.

Conclusions

In the opinion of the authors, the content of the article may be a starting point for further research, e.g. directed at the decision-making process in crisis situations or answering the question: what to do and in what order in the event of a crisis situation?

The results of the study highlight the importance of information and time in crisis management. They emphasise the need not only to have certain knowledge, but also the validity of using it in the shortest possible time. This view of the issues is appropriate because adverse events have their own dynamics. When forecasting the development of the situation and taking appropriate actions, it is necessary to strive to ensure that information and time serve well for the return to the state of normality, where security will be a category and condition beneficial for society and the environment.

Acknowledgement

No acknowledgement and potential founding was reported by the authors.

Conflict of interests

All authors declared no conflict of interests.

Author contributions

All authors contributed to the interpretation of results and writing of the paper. All authors read and approved the final manuscript.

Ethical statement

The research complies with all national and international ethical requirements.

ORCID

Zenon Zamiar https://orcid.org/0000-0001-9887-0183

Zbigniew Ścibiorek https://orcid.org/0000-0002-7408-4302

References

1. Moczydłowska JM. *Potencjał kompetencyjny pracowników jako źródło zmian w strategii organizacji*. In: Szabłowski J (ed.). *Zmiany w strategiach zarządzania organizacjami*. Białystok: Wyższa Szkoła Finansów i Zarządzania; 2009, p. 311-324.
2. *Słownik języka polskiego. T. 3*. Warszawa: Państwowe Wydaw. Naukowe; 1981.
3. Majer P. *W poszukiwaniu uniwersalnej definicji bezpieczeństwa wewnętrznego*. Przegląd Bezpieczeństwa Wewnętrznego. 2012;7(4):11-18.
4. Grudzewski WM, Hejduk I (eds.). *Przedsiębiorstwo przyszłości*. Warszawa: Difin; 2000.
5. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. Nr 89, poz. 590 z późn. zm.).
6. Kuc BR, Żemigała M. *Menedżer nowych czasów. Najlepsze metody i narzędzia zarządzania*. Gliwice: Helion; 2012.
7. Modrzejewski Z. *Militarne obszary komunikacji strategicznej*. Warszawa: Akademia Sztuki Wojennej; 2020.
8. Kisielnicki J, Sroka H. *Systemy informacyjne biznesu*. Warszawa: Placet; 2005.
9. Ścibiorek Z. *Decydowanie podstawową funkcją zarządzania*. Toruń: Wydawnictwo Adam Marszałek; 2021.
10. Sumpter D. *Osaczeni przez liczby. O algorytmach, które kontrolują nasze życie. Od Facebooka i Googla po fake news i bańki filtrujące*. Warszawa: Copernicus Center Press; 2019.
11. Makowski M. *W niewoli mass mediów*. In: Bąk K, et al. Rybakiewicz J (ed.). *Człowiek i psychologia*. Bielsko-Biała: Park; 2004, p. 339-45.
12. Kacała T. *Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa*. Przegląd Prawa Konstytucyjnego. 2015;2(24):49-65.

13. Szczupaczyński J. *Anatomia zarządzania informacją*. Warszawa: Międzynarodowa Szkoła Menadżerów; 1998.
14. Woźniak-Kasperek JB. *Przeciążenie informacyjne – sprawozdanie do tematu*. Fides Biuletyn Bibliotek Kościelnych. 2018;2(47):77-92.
15. Fritz R. *ABC nowoczesnego menedżera*. Pulnar P (transl.). Warszawa: Wydawnictwo AMBER; 2002.
16. Łukasiewicz R. *Rozwój informatyczny a cyberterroryzm*. In: Hołyst B, Jałoszyński K, Letkiewicz A (eds.). *Wojna z terroryzmem w XXI wieku*. Szczytno: Wydawnictwo Wyższej Szkoły Policji; 2009.
17. Nepelski M. *Przestrzeń wirtualna w procesie kompresji zagrożeń. Rozprawa habilitacyjna* [dissertation]. Warszawa: Akademia Obrony Narodowej; 2013.
18. Szubrycht T. *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*. Zeszyty Naukowe Akademii Marynarki Wojennej. 2005;1(160):173-87.

Biographical note

Zenon Zamiar – Col. (ret.), Prof. Dr. hab. Eng., Former dean and vice-rector at the Military University of Land Forces. Currently Vice-Rector at the International University of Logistics and Transport in Wrocław. Research areas: security, crisis management, crisis logistics.

Zbigniew Ścibiorek – Col. (ret.), Prof. Dr. hab. Eng., Former Deputy Dean of the Faculty of Management and Command of the National Defense University. Currently a full professor at the International University of Logistics and Transport in Wrocław. Research areas: geopolitical situation, management and command, as well as on the methodology of security sciences.

Rola informacji w zarządzaniu kryzysowym

STRESZCZENIE W artykule zaakcentowano, że obecne warunki dotyczące monitorowania i zapewnienia bezpieczeństwa wewnętrznego są coraz bardziej złożone. Złożoność wielu procesów i ich trudne uwarunkowania akcentują potrzebę dokonywania w miarę szybkich rozstrzygnięć. W ślad za tym wymogiem znacznie więcej uwagi poświęca się poprawie funkcjonowania systemów informacyjnych. Podkreślono, że coraz większa ilość informacji z jednej strony jest zjawiskiem korzystnym, ale z drugiej strony nie zawsze sprzyja podjęciu w miarę szybkiej decyzji. Trzeba dążyć do zdobywania różnymi kanałami (sposobami) wiarygodnej informacji, która będzie podstawą dokonywania rozstrzygnięć oddalających zagrożenia bezpieczeństwa i (lub) minimalizujących jego skutki. Podkreślono, że droga do osiągnięcia założonych celów jest w każdym przypadku odmienna; nie można przedstawić uniwersalnej metodyki postępowania. Oprócz uwarunkowań przedstawiono szereg propozycji ukierunkowanych na doskonalenia działalności osób sprawujących funkcje kierownicze oraz funkcjonowanie zespołów zarządzania kryzysowego.

SŁOWA KLUCZOWE bezpieczeństwo, bezpieczeństwo wewnętrzne, zarządzanie kryzysowe, informacja

How to cite this paper

Zamiar Z, Ścibiorek Z. *The role of information in crisis management*. Scientific Journal of the Military University of Land Forces. 2022;54;2(204):245-55. DOI: 10.5604/01.3001.0015.8976.