
Case Study Method as an Interdisciplinary Approach to the Issue of Estimating the Security Level

Submitted 07/11/21, 1st revision 02/12/21, 2nd revision 24/12/21, accepted 22/01/22

Milena Palczewska¹, Grzegorz Pilarski²

Abstract:

Purpose: The article presents the case study method, which allows the use of an interdisciplinary approach to multi-faceted estimation of the security level (in various dimensions).

Design/Methodology/Approach: Due to numerous threats, forecasting, as rational, scientific, predicting future events, i.e., inferring about unknown events based on known events, has become an important element of security sciences. It allows to predict future events with high probability and thus effectively react in a crisis or conflict situations.

Findings: 21st century has been dominated by information technologies, and information itself is becoming an extremely valuable resource. Therefore, main finding is method of estimating the level of security - scheme of analysis (eight stages) of any potential threat, incident or phenomenon in the scope of security level estimation.

Practical implications: The content of the article can be useful to theorists and practitioners who are concerned with security in all dimensions.

Originality value: State security is a derivative of many different - individual and group - values in the field of security. Security, however, cannot be seen as the algebraic sum of the security of individuals and social groups, and international security as the sum of the security of individual states. A nation perceives its security through the prism of challenges and threats caused by conflicts that occur in a given society or its neighbourhood.

Keywords: Security, interdisciplinarity, case study method.

JEL codes: Security issues.

Paper type: Research article.

¹Assoc. Prof. PhD., War Studies University, Poland, m.palczewska@akademia.mil.pl;

²Assoc. Prof. PhD., War Studies University, Poland, g.pilarski@akademia.mil.pl;

1. Introduction

Security can be considered in many dimensions, national, international, internal, social, economic, ecological, cultural, etc. It is important to correctly estimate the level of security, as it affects the proper functioning of organizations, societies and states. Therefore, the aim of the article is to define the foundations of security in the objective and subjective dimension, and to indicate the interdisciplinary nature of the issues related to security. Moreover, the aim is to present a case study method in relation to the security level estimation.

Therefore, the main research problem is: How to estimate the level of security using the case study method? With the adopted research assumptions, it was possible to formulate the main theses in the article, which are based mainly on theoretical research methods. Its content can be of useful to theorists and practitioners who are concerned with security in all dimensions.

Security is still shaped by the progress of civilization, which is why the society poses even greater expectations of the state in relation to ensuring security. Security also means securing yourself and your loved ones against any threats that occur during real danger or danger. The level of security must meet many requirements set by the state as a key authority that builds, supervises, controls and, if necessary, modifies the overall system.

However, national security is not only about protection and defense, but also about the existence of the state as such, which guarantees the successful existence and development and protection of the values of individual members of the community. It is worth emphasizing that the sense of security for individuals is the most important, which is why many countries and international organizations focus on creating an appropriate security condition. Security, in fact, depends primarily on what is happening around our environment, both internal and external, because potential threats can come from there. The society must be prepared for threats, therefore the authorities must prepare units to react quickly and combat a threat at the beginning of its emergence.

2. Interdisciplinarity of Security - Basic Assumptions

The key issue of this article is to present and define the generally understood concept of security. The term "security" is derived from the Latin word *sine cura = securitas* (without custody). In the colloquial understanding, security is understood as the absence of threats, while in dictionary definitions the most common approach is the term that identifies the term security with certainty, a state that is opposed to threats. So security means the same as freedom from threats³. At this point, it is necessary to

³*Veľas, A., Halaj, M., Hofreiter, L. et al. Research of security and safety culture within an organization. The case study within the Slovak Republic. Security Journal (2021).*

introduce the concept of securitology as a distinguished scientific discipline, which aims to research all threats to the existence, development and proper functioning of the individual, as well as social organizations. Securitology is a new science about human security, which dates back to the 90s of the twentieth century. The subject matter of the above-mentioned scientific discipline covers a number of cultural, sociological, legal and political factors that have a significant impact on threats.

If we talk about a dynamic phenomenon (process) of security of a given entity in a practical sense, we mean the area of its activity that aims to ensure the possibility of survival, development and the freedom to pursue one's own interests in specific conditions, by taking advantage of favorable circumstances (opportunities), taking up challenges, reducing risk and counteracting (preventing and opposing) all kinds of threats to the entity and its interests.

All kind of threats are the source of searching and expanding knowledge on security. As part of its deliberations, the science of security deals with the problem of researching threats that, by the fact of their occurrence, threaten the existence, development, normal functioning of each individual and all social organizations. The concept of security should be considered in two main approaches, namely, subjective and objective. The subjective aspect of security relates to people. By this we mean the safety of individual individuals, groups of people and all kinds of organizations that have a formal character and are territorially located in administrative and state structures, e.g. municipalities, voivodships, national level and collectives of states.

In the above situation, security should be considered in analogous aspects, local, national and international security⁴. The subjective approach to security is understood in the context of security, military, political, economic, ecological, social and cultural. Security can be considered as a certain state, feeling, process, goal, value, need, structure. When analyzing the aspect of national security, the priority is to study the relations between the state and the citizen. The foundation of these is the developed system of values, general norms, beliefs and attitudes. Security is treated in highly developed countries as a public good.

It is necessary to strive for a situation in which there would be no situation where, at the expense of one entity, another entity loses its security. A state of relative security should be guaranteed to all citizens residing in a given country. Due to the dynamics of threats, states that want to provide their citizens with a sense of security face the challenge of engaging in the creation and development of international security, which is the result of complex processes of globalization and interactions between actors playing a role on the political and economic scene.

⁴*Spadaro G, Gangl K, Van Prooijen J.W, Van Lange PAM, Mosso CO (2020) Enhancing feelings of security: How institutional trust promotes interpersonal trust. PLoS ONE 15(9).*

Security as a scientific discipline has been practiced relatively recently in many universities, both public and private. It is also the subject of many international conferences and symposiums. The issue of security in the face of the emergence of new threats is constantly gaining importance both in the national and local level and in the international dimension. Security is a dynamic concept. It is undergoing constant processes of change. This is due, on the one hand, to the constantly emerging threats that threaten peace and stability. While second significant factor is the growing phenomena and processes that intensified at the end of the 20th century, including, the decay of the bipolar world, the superpower position of the United States of America, globalization, scientific and technical progress, IT revolution, development of world terrorism.

Taking into account new phenomena and processes, the main security problems that will occur in the future should be indicated to:

- radical changes in defense, foreign and intelligence policies;
- adopting a new international strategy against terrorism;
- effective action in crisis situations;
- the effectiveness of the peace settlement system;
- building a cooperative security model;
- multilateral cooperation as a mean of strengthening peace;
- limiting the number of countries in access to weapons of mass destruction⁵.

At this point it should be indicated that the subject of research in the security sciences are all modern security systems that cover the military and non-military dimensions. All of these systems work within institutions that are state and local government, or are independent enterprises or social organizations. Research that is carried out in the field of the scientific discipline of security should focus on creating theoretical foundations for the development of security systems. Undoubtedly, the subject of considerations of security science should be the functioning of the state and all international organizations.

All this should lead to the goal of ensuring national and global security. Within this scientific discipline of security sciences, the following research problems should occur: security theory, security history, global security, national security, public security, social security, economic security, security policy, identification and assessment of threats on a global and national scale, identification and management of crisis situations, design and evaluation of security systems, international terrorism, methodology of security research⁶.

⁵Douglas B Atkinson, Joshua Jackson, George W Williford, *Rivalry, Uncertainty, and Militarized Compellent Threats*, *Journal of Global Security Studies*, Volume 6, Issue 1, March 2021.

⁶Venema, L. *Defining a role for AI ethics in national security*. *Nature Mach Intell* 3, 370–371 (2021).

Referring directly to the topic of the article, it is necessary to indicate the dimensions in which security can be considered. It is interdisciplinary and affects practically every area of human functioning. There are the following types of security:

- due to the area it covers - global security, international security, regional security, national security;
- due to the attitude to the territory of the state - external and internal security;
- due to the field in which it occurs - ecological, economic, energy, physical, IT (cyber), cultural, military, political, social security and identification security⁷.

3. Case Study Method

On the basis of a four-stage forecasting process presented by J.E. Russo and P.J.H. Schoemaker⁸ as well as the incident probability range proposed by P.E. Tetlock and D. Gardner⁹ and last but not least the four uncertainty levels by H.G. Courtney, J. Kirkland and S.P. Viguerie¹⁰, the authors propose to adopt the following scheme of analysis (eight stages) of any potential threat, incident or phenomenon in the scope of security level estimation.

Identification of the analyzed case – a clear-cut forecasting objective, identification of the basic assessment indicators, the choice of core reality description parameters. In this part of the analysis it is necessary to uniquely determine the research problem in the form of a question which we strive to find the answer to e.g.: Is it possible to carry out an effective cyber attack on the critical energy infrastructure in Warsaw till the end of year 2022? In this part it has to be stated precisely what is the exact aim of the analysis. In the above mentioned case it is required to define what an effective cyber attack means e.g. it will be the one which results in a blackout for a period of time exceeding two days. The next element to be determined can be the specification what exactly is entailed in the critical energy infrastructure, etc. The aim of all the activities is the so called framing to uniquely determine the key analysis elements of the surrounding reality of the subject research problem.

General description of the analyzed case – in this part it is required to gather information on the analyzed issue. The outcome of the analysis is in the form of a comprehensive description of the problem or the assessed country.

⁷Azzuni, A.; Breyer, C. *Global Energy Security Index and Its Application on National Level*. *Energies* 2020, 13, 2502.

⁸J.E. Russo, P.J.H. Schoemaker, *Winning decisions: Getting it right the first time*, Currency Doubleday, New York 2002, pp. 1 – 17.

⁹P.E. Tetlock, D. Gardner, *Superforecasting: the art and science of prediction*, Crown Publisher, New York 2015, pp. 47 - 81.

¹⁰H.G. Courtney, J. Kirkland, S.P. Viguerie, *Strategy under uncertainty*, McKinsey Quarterly 2000.

Initial indication of uncertainty level for the examined case – on the basis of the gathered information, the analyst performs an initial assessment of the uncertainty level of the analyzed research problem. The analysis is then taken into consideration in point six to estimate the security level of the analyzed case. In this part it is very useful to apply averaged experts' forecasts and weight functions for the obtained experts' opinions¹¹. The more reliable expertise obtained on the basis of the gathered information, the higher weight function is applied. Table 1 presents the example of statistical data depiction. The example shows four probability indicators. The first one as the base rate of analysis is a subjective assessment of the analyst who examines the given research problem. Sometimes the value amounts to 50% which means that the analyzed phenomenon can happen or not with the equal probability for both cases. Moreover, the table provides percentage indicators for three experts' opinions.

Table 1. Statistical data of the initial uncertainty level

Source	Iteration I	Iteration II
Base rate of analysis	%	
Expertise 1	%	
Expertise 2	%	
Expertise 3	%	x3
	% /4	% /6
Probability	%	%

Source: Own elaboration.

What is characteristic for each expert's opinion is the fact that the information can be obtained from different sources. The more reliable source of expertise, the closer it is to the expected level of uncertainty for a given case, in the opinion of the analyst. The probability calculation is done in two iterations. The first one provides averaged result of the base rate and the experts' forecasts, in our case the sum of four analyses is divided by four. Whereas in the second iteration, the third expertise was given weight function three. As a result, the average result is obtained by multiplying the third expertise by three.

In our case, the sum of base rate probability for the first, the second, and three values of the third expertise is divided by six. In this method the sources of information can be taken more or less precisely. The more reliable source, the more exact results. What is more, the sheer base rate is of significant importance, still the indicator can be of different value depending on the initial knowledge about the analyzed issue, which in turn contributes to more precise initial estimation.

General economic, social and political analysis of the examined case – in this part it is required to gather information concerning chosen aspects of economic

¹¹Bernstein, P.L., *Against the Gods, the remarkable story of risk*, John Wiley & Sons, Inc., New York 1998, pp. 50 - 53.

analysis of the area affected by the analyzed issue. The forecast may involve answers to the following questions: what is the economic situation of a given country, is the country on the correct or incorrect course, can the change of the economic situation affect the analyzed problem. The analysis can be extended by political and social issues if the case is to be described with respect to those spheres. The above mentioned aspects are given only as examples, the analyst individually determines which aspects will be taken into consideration in a given analysis, depending on the research problem or the needs expressed by the decision maker.

Chosen analytical techniques – in this part the gathered information is analyzed with the use of varied, available tools e.g., comparative foreign policy analysis¹²; averaging experts' forecasts¹³; game theory¹⁴; scenarios analysis¹⁵ etc. Scenarios analysis is an interesting technique. In terms of this analysis it is required to indicate probable actors participating in a scenario, set the indicators (positions) of a phenomenon impact (Table 2.) and create a matrix of dependencies and impact of actors/players (Table 3.). The technique allows to determine the level of probability that the analyzed incident will take place.

The indicators of a phenomenon impact are the parameters which are subjectively determined by the analyst, depending on the analyzed phenomenon, through assigning a given value to the probable state. As a rule, extreme values are assigned to the opposite states e.g., '100' for the phenomenon taking place and '0' for the phenomenon not taking place.

Table 2. Exemplary indicators of a phenomenon/incident impact

Position (P)	Probable states
100	incident will not take place
70	low emergency state
50	medium emergency state
30	high emergency state
0	incident will take place

Source: Own elaboration.

¹²J.S. Lantis, R. Beasley, *Comparative Foreign Policy Analysis*, Oxford Research Encyclopedias 2017, available on: <https://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-398> [accessed June 2021], DOI: 10.1093/acrefore/9780190228637.013.398.

¹³P.L. Bernstein, *Against the Gods, the remarkable story of risk*, John Wiley & Sons, Inc., New York 1998, pp. 50 - 53.

¹⁴Bonanno G., *Game theory*. 2nd Edition, Department of Economics, University of California 2018, Davis, access on: http://faculty.econ.ucdavis.edu/faculty/bonanno/PDF/GT_book.pdf [accessed June 2021].

¹⁵R. MacKay, P. McKiernan, *Scenario Thinking: A Historical Evolution of Strategic Foresight (Elements in Business Strategy)*, Cambridge: Cambridge University Press 2018. DOI:10.1017/9781108571494.

Table 3. Matrix of dependencies and actors/players impact

Actor/ player	Position (P)	Saliency (S)	Impact (I)	I*S	I*P	I*S*P
Actor 1	100					
Actor 2	100					
Actor 3	100					
Actor 4	50					
Actor 5	70					
Actor 6	0					
Actor 7	30					
Actor 8	30					
Sum						

Source: Own elaboration.

In the above matrix, the probable actors are assigned certain indicators in accordance with Table 2 (Position – P). Additionally, on the basis of the gathered data the analyst subjectively assesses and assigns certain values from the scope of 0-100 to the ensuing parameters describing actors/players, i.e., their saliency (S) and their impact (I) in the scope of the analyzed incident. The next columns provide the results of arithmetic operations.

Through the analysis of the results obtained on the basis of a percentage probability distribution it is possible to make calculations for given positions by computing the probability of a given state occurrence (Table 4).

Table 4. Exemplary data – probability of a given state occurrence

Possible states	Position	Impact	Probability
incident will not take place	100		%
low state of emergency	70		%
medium state of emergency	50		%
high state of emergency	30		%
incident will take place	0		%

Source: Own elaboration.

For that purpose, it is required to sum up the results of operation I*S (Table 3) for a given position and then divide it by the sum of all results of the operation. For position ‘100’ (incident will not take place) there are three actors for whom we sum up the values from column I*S and then we divide it by the result of the sum for all the results of the operation. Next, we divide the obtained value by the sum of all result of operation $\Sigma I*S$ (Table 3) and it gives a percentage value of the estimation if a given state will take place. The calculation is done for all possible states of a position (P). Next, on the basis of subsequent calculations from Table 3 it is possible to determine the zone of possible results, i.e., the possible states in the discussed case. The scope begins with the highest probability value presented in Table 4.

The end of the scope has to be calculated with the use of a weight function in accordance with the following formula $\Sigma (I*S*P) / \Sigma (I*P)$. The obtained result is the basis for the estimation which indicator is the closest to the given calculated value. The exemplary data is compared in Table 5.

Table 5. *Exemplary data – zone of possible outcomes*

Probability	%	%	%	%	%
Position	100 incident will not take place	70 low state of emergency	50 medium state of emergency	30 high state of emergency	0 Incident will take place
Zone of possible outcomes	x	x			

Source: Own elaboration.

In the above presented case, the scope of the possible outcomes zone entails two states, 100 and 70 which might imply that there is a high probability that the incident will not take place but it is advised to take into consideration a low emergency state.

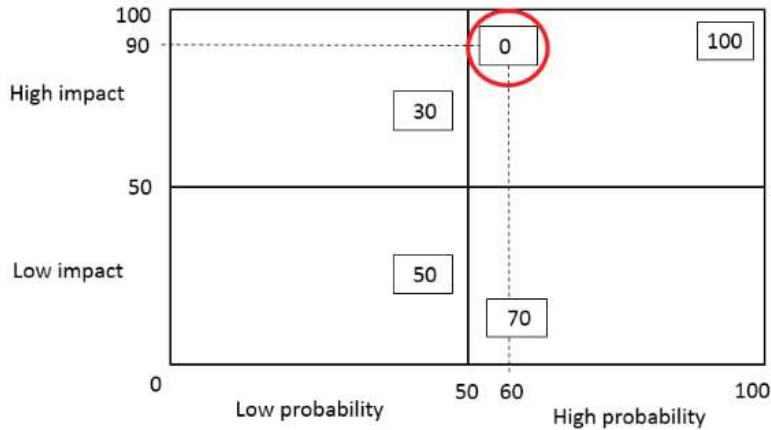
The next analytical tool which can be applied is the risk matrix – the matrix of dependencies between the probability of a given state (position) occurrence and the resulting impact. The analyst uses the gathered data to assess the level of probability that a given state (position) will occur alongside with any potential damage (impact) which might be observed in case the state appears. Figure 1 presents an example of a risk matrix with five possible probability states. In the course of the analysis it is important to determine the conditions under which the analyzed incident can take place, thus the focus is on position ‘0’.

Figure 1 shows that the analyzed case is characterized by the probability value of about 60% and the impact of about 90%. The given values allow to estimate the risk of the state occurrence through the product of the probability and the impact. Another interesting tool for analysis are casual loop diagrams which allow to visualize the analyzed phenomena. This graphic solution reveals relations between the elements of an organization or a system¹⁶, which can remain unseen in the

¹⁶M. Goodman, *Systems thinking: what, why, when, where, and how?*, Systems thinker by Pegasus Communications 2018, access on: <https://thesystemsthinker.com/systems-thinking-what-why-when-where-and-how/> [accessed June 2021].

description of an analyzed case. The diagrams provide a language to express our understanding of the dynamic, correlated nature of the world¹⁷.

Figure 1. The example of a risk matrix



Source: Own elaboration.

Estimation of security level for the analyzed case – in this part of the analysis it is required to aggregate the obtained results in order to assess the probability of the examined case occurrence. In order to achieve this goal it is necessary to average the results regarding the analysis base rate as well as the results obtained with the use of certain analytical techniques (Table 6).

In the above mentioned example there are four results of the analysis: the analysis base rate and three probability values obtained through the applied analytical techniques.

Table 6. Statistical data of the estimated security level

Source	Iteration I	Iteration II
Base rate of analysis	%	
Analysis 1	%	x3
Analysis 2	%	
Analysis 3	%	
	% /4	% /6
Probability	%	%

Source: Own elaboration.

It is possible to carry out any number of analyses depending on the time and the resources used to prepare the forecast. Similarly to point three, it is possible to apply iteration and assign certain weight functions to results which are most reliable in the opinion of the analyst.

¹⁷Kim, D.H., 1994. *Systems thinking tools. A user's reference guide*, Pegasus, Waltham, pp. 18 - 21.

Forecast reliability – in this part of the analysis, taking into consideration the obtained probability results it is possible to determine the level of confidence regarding the analyzed case. For that purpose, it is advised to apply scopes of probability proposed by P.E. Tetlock and D. Gardner¹⁸. Additionally, taking into consideration the levels of uncertainty¹⁹ by H.G. Courtney, J. Kirkland and S.P. Viguerie it is possible to determine the reliability of the analyzed case forecast.

Iternative forecast outcomes – in this part of the analysis it is possible to indicated alternative cases which might appear, even those most unlikely.

4. Conclusion

There is no doubt that the 21st century has been dominated by information technologies, and information itself is becoming an extremely valuable resource. The dynamic development of information and communication technologies accompanying economic and social processes means that the functioning of individual areas of modern countries is increasingly dependent on access to information and uninterrupted operation of technical infrastructure²⁰. Security and forecasting are also undeniably associated with it. Therefore, in the presented method of estimating the level of security, scientific rational prediction was used - inference is a logical process running from the collection of facts from the past with the use of scientific methods²¹.

The above proposal is a tool which allows to estimate the level of security in a fairly short period of time. The authors believe that the assessment of security is a vital topic since it provides the decision makers with information expressed in numbers or in averaged percentage values. It should be stressed that in that type of analysis more than half of the time is spent on the realization of two stages, namely, framing and gathering intelligence data²². The stages are mostly based on gathering confirmed facts, historical data, etc., thus, it is very important to choose reliable data in order to obtain reliable security assessment. It is advisable that the presented methodology of security level estimation can be used by a wide group of security theorists and

¹⁸P.E. Tetlock, D. Gardner, *Superforecasting: the art and science of prediction*, Crown Publisher, New York 2015, pp. 47 - 81.

¹⁹H.G. Courtney, J. Kirkland, S.P. Viguerie, *Strategy under uncertainty*, McKinsey Quarterly 2000.

²⁰G. Pilarski, *The Concept of Recommender System Supporting Command and Control System in Hierarchical Organization*, 2014 European Network Intelligence Conference, 2014, 33 (33) pp. 138-141, doi: 10.1109/ENIC.2014.9.

²¹G. Pilarski, *How to Estimate Security – Problem Analysis*, *Security Dimensions*, 2020, pp. 217-240, doi: 10.5604/01.3001.0014.2678.

²²J.E. Russo, P.J.H. Schoemaker, *Winning decisions: Getting it right the first time*, Currency Doubleday, New York 2002, pp. 1 – 17.

practitioners. The idea of the interdisciplinarity of this method allows it to be used in practically every security dimension - cyber, military, social or economic.

References:

- Atkinson, D.B., Jackson, J., Williford, G.W. 2021. Rivalry, Uncertainty, and Militarized Compellent Threats. *Journal of Global Security Studies*, 6(1).
<https://doi.org/10.1093/jogss/ogz079>.
- Azzuni, A., Breyer, C. 2020. Global Energy Security Index and Its Application on National Level. *Energies*, 13, 2502. <https://doi.org/10.3390/en13102502>.
- Bernstein, P.L. 1998. *Against the Gods, the remarkable story of risk*. John Wiley & Sons, Inc., New York, pp. 50-53.
- Bonanno, G. 2018. *Game theory, 2nd Edition*. Department of Economics, University of California.
- Courtney, H.G., Kirkland, J., Viguerie, S.P. 2000. *Strategy under uncertainty*. McKinsey Quarterly.
- Goodman, M. 2018. *Systems thinking: what, why, when, where, and how? Systems thinker by Pegasus Communications*. Available online:
<https://thesystemsthinker.com/systems-thinking-what-why-when-where-and-how/>.
- Kim, D.H. 1994. *Systems thinking tools. A user's reference guide*. Pegasus, Waltham, 18-21.
- Lantis, J.S., Beasley, R. 2017. *Comparative Foreign Policy Analysis*. Oxford Research Encyclopedias. DOI: 10.1093/acrefore/9780190228637.013.398.
- MacKay, R., McKiernan, P. 2018. *Scenario Thinking: A Historical Evolution of Strategic Foresight (Elements in Business Strategy)*. Cambridge: Cambridge University Press. DOI:10.1017/9781108571494.
- Pilarski, G. 2014. The Concept of Recommender System Supporting Command and Control System in Hierarchical Organization. *European Network Intelligence Conference*, 33(33), 138-141. DOI: 10.1109/ENIC.2014.9.
- Pilarski, G. 2020. How to Estimate Security – Problem Analysis. *Security Dimensions*, 217-240. DOI: 10.5604/01.3001.0014.2678.
- Russo, J.E., Schoemaker, P.J.H. 2002. *Winning decisions: Getting it right the first time*. Currency Doubleday, New York, pp. 1-17.
- Spadaro, G., Gangl, K., Van Prooijen, J.W., Van Lange, P.A.M., Mosso, C.O. 2020. Enhancing feelings of security: How institutional trust promotes interpersonal trust. *PLoS ONE*, 15(9). <https://doi.org/10.1371/journal.pone.0237934>.
- Tetlock, P.E., Gardner, D. 2015. *Superforecasting: the art and science of prediction*. Crown Publisher, New York, pp. 47-81.
- Veľas, A., Halaj, M., Hofreiter, L. et al. 2021. Research of security and safety culture within an organization. The case study within the Slovak Republic. *Security Journal*. <https://doi.org/10.1057/s41284-021-00291-5>.
- Venema, L. 2021. Defining a role for AI ethics in national security. *Nature Mach Intell*, 3, 370-371. <https://doi.org/10.1038/s42256-021-00344-9>.