Vojtech Jurčák – Ján Mišik[1]

Risk Analysis

After the end of the bipolar world, the security environment is increasingly complicated, characterised by instability and uneven development, as well as high dynamics. The instability and uneven development of the security environment is caused by insufficient solutions to the world's global problems. The complexity of the security environment creates problems in characterising the current security actors, which are not only traditional states as the main security actors but also non-state actors, possessing weapons that in the past were owned only by superpowers. During the Cold War we knew the intentions of individual actors but did not know their potential or secret facts, but currently the opposite is true. We know the available capacities, but we do not know the intentions of the actors acting in a given security environment with unconventional means for unconventional goals and using asymmetric strategies to achieve their goals. The possibilities of destabilising the state, affecting the population, or destroying an element of critical infrastructure are no longer a matter of using strategic nuclear carriers, large-scale operations, but include laptops, computer networks, smuggled chemical, biological, radioactive substances, targeted propaganda, organised crime, etc.

Different definitions

There are several different definitions of a hybrid threat. An important sign when a threat becomes a hybrid is its use in combination with another type of threat to achieve a synergistic effect together and achieve one common goal. If a state or non-state actor wants to act on another actor and achieve its goals, it chooses the means and forms of hybrid warfare from its available resources and deploys them against its adversary. This adversary perceives deployed resources or resources that may be deployed in the future as threats to its security. If these resources are a combination of conventional forces, non-conventional forces, terrorist activities, criminal activities and various combinations of political, economic, social

[1] Armed Forces Academy of General Milan Rastislav Štefánik.

DOI: https://doi.org/10.36250/01195_09

and informational activities and tools, then they become a hybrid threat. In this sense, the deployment of regular conventional military force is also a hybrid threat. It is enough if it cooperates, for example, with the means of information warfare. It follows that any security threat in the classical sense can become a hybrid threat.[2] The terms threat and risk are used interchangeably in practice. In general, we use the terms security threats and risks to express undesirable phenomena of a natural and social nature that can potentially damage protected values. These words are very similar and their content is the subject of debate in professional circles. For the purposes of this topic, the relationship between them can be expressed by the term complementary approach. The essence of this approach is the use of risk to express the acuteness of the threat.[3] This approach emphasises the relationship between risk and uncertainty. The European Union (EU), which considers the issue of hybrid threats a challenge for the current security in Europe, in its document "Common Framework for Combating Hybrid Threats" provides one of the most comprehensive definitions of hybrid threats. The EU defines the objective of the hybrid threat as follows: "The aim is not only to cause direct losses and exploit weak points, but also to destabilize society and provoke uncertainty that is intended to paralyze decision-making processes."[4] Security actors encounter various external and internal factors and influences that create uncertainty as to whether and when they will achieve their goals. The negative effect that this uncertainty has on the intentions (goals) of the actor – reference object represents a security risk.[5] The risk arises because these intentions will be monitored in the light of uncertainties. Uncertainty or lack of it is a state of, even if partial, lack of information that relates to understanding or knowledge about an event, its consequences or possibilities. This condition leads to inadequate or incomplete knowledge or understanding of the event, its consequences or probability. Therefore, it is necessary to reduce uncertainty as much as possible. Actors can set their intentions or goals, but to achieve them they often have to struggle with internal and external factors that they may not influence and that create uncertainty and thus risk. These factors can prevent or delay their achievement. Security risks, whose assessment process

2 Jurčák et al. 2017.
3 Laml 2008.
4 European Commission 2016: 14.
5 ISO 31000.

(identification, analysis and evaluation) is the subject of this topic, result from a certain danger called a hybrid threat. Risk management represents coordinated activities to manage and control the actor with regard to risk. It contributes to the understanding of the possible disadvantages of all factors that affect the actor and helps in decision-making by taking into account the uncertainty and possibilities of future events or circumstances (planned or unplanned) and their consequences for the chosen goals. A well-executed identification, analysis and assessment of security risks will make it possible to find appropriate ways to deal with permissible and unacceptable risks, which need to be modified and monitored in a certain way so that they do not cause serious negative consequences. Considering the nature of the sources of security risk consisting in a hybrid threat, it is necessary to assess each risk first individually and then in mutual contexts to determine priorities and consider a possible domino effect.[6] Sources of risk in individual areas of the security sector can be derived from the means used to conduct hybrid warfare as follows:[7]

- military
- political
- economic
- financial
- cybernetic
- propaganda
- diplomatic
- media
- symmetric
- terrorist
- etc.

The first part of the chapter focuses on the characteristics of the stages of risk assessment, including the methods that can be used. The second part is dedicated to the possibility of using modern computer technologies in the process of risk management.

6 ISO 31000.
7 ISO 31000.

Risk assessment

Risk assessment is a part of risk management that provides a structured process for identifying how the security actor's objectives may be affected and for analysing risks in terms of consequences and likelihood before deciding whether further risk management is necessary. When assessing risks, the following fundamental questions must be answered:[8]

- What can happen and why (using risk identification)?
- What are the consequences?
- What is the probability of their future occurrence?
- Are there any factors that mitigate the consequences of the risk or that reduce the likelihood of the risk?
- Is the level of risk permissible or acceptable and does not require further treatment?

There are several different risk assessment methodologies that can be used for individual risks arising from hybrid threats, e.g.:[9]

- RAM (Risk Assessment Methodology)
- RVA (Risk and Vulnerability Analysis)
- RAMCAP (Risk Analysis and Management for Critical Asset Protection)
- VAM (Vulnerability Assessment Methodology)
- Risk Assessment FEMA (Federal Emergency Management Agency)
- etc.

Management systems built on the basis of Annex SL (e.g. ISO 27000, ISO 14000, ISO 9000) refer to the ISO 31000 standard at the planning stage, which provides universal principles, structure and guidance for risk management. If, for example, we will deal with information security risks – the attack vector, so the ISO 31000 standard – will allow us to work with risks in other areas as well. The risk assessment according to this standard is given as follows. According to ISO 31000 risk assessment is an aggregate process:[10]

- Risk identification – a process used to find, examine and describe risks that could affect the achievement of goals (objectives).

[8] ISO 31000.
[9] ISO 31000.
[10] ISO 31000.

- Risk analysis – a process that is used to understand the nature, sources and causes of risks to determine and assess the level of risk, it is also used to investigate their impacts and consequences and survey the established risk management measures.
- Risk assessment – a process used to compare the results of risk analysis with risk criteria and decide on risks that require treatment.

The process of risk management must begin by defining what we want to achieve – the required level of security (protection), and to understand the external and internal factors that can affect success in achieving the goals. This step, called "contextualisation", necessarily precedes risk identification. In addition to the analysis of the external and internal security environment, the contextualisation stage also includes the definition of risk criteria.[11]

Risk identification

Risk identification means the process of finding, recognising and describing the risk. Risk identification includes finding out:[12]

- Sources of risk – elements that by themselves or in combination have the internal potential to cause risk and the areas of their consequences. This includes events that risk sources can cause and circumstances that could have potential consequences for security.
- Causes of risk – answer the questions of what can happen, when and where, why and how it can happen.
- Potential consequences – include measures introduced to modify the risk.

The aim of risk identification is to create a comprehensive list of risks, based on events that could prevent, invalidate or delay the achievement of objectives to achieve, ensure, support and build security at the required level. The purpose of risk identification is to find out what could happen or what situations could occur that could affect the achievement of security objectives. As soon as the risk is identified, the actor should identify possible suitable measures for its modification, such as mechanical restraints, closed-circuit televisions (CCTV),

[11] ISO 31000.
[12] ISO 31000.

regime measures, physical protection and others. These measures are listed in the risk list. Exhaustive identification must be critical because risks not identified at this stage will not be included in further analysis. Subsequently, these risks cannot and will not be modified or otherwise influenced. The actor should use risk identification tools and techniques that correspond to his capabilities as well as the occurring risks. People with appropriate knowledge and experience should be involved in the identification of risks. Current and relevant information is important in risk identification, and if possible, should include appropriate feedback information. Risk identification can use:[13]

- historical data
- theoretical analyses
- opinions of informed persons and experts
- needs of interested participants

The identification of sources of risk or source identification means the process of finding, recording and describing the elements that alone or in combination have the intrinsic potential to cause risk and the areas of their consequences. If the source or problem is known, the events that may be raised by the source or events can be resolved. Methods (techniques) of risk identification. The following groups of techniques (methods) can be used to identify risks:[14]

- Deductive methods (ex-post methods) or evidence-based methods – are based on the analysis of events that have already occurred, the search for and clarification of their causes and connections between them. The last event is considered and the circumstances that could have caused it are sought. They can be used to create scenarios for the emergence and manifestation of various risks, they are a source of innovation in safety management processes.
- Inductive methods (ex-ante methods) – they allow predicting possible risks for protected assets, while analysing sources that could cause negative events. Using these methods, it is possible to evaluate the expected (expected, probable) number of events, estimate their possible consequences and take appropriate preventive measures. Inductive methods generally use:

[13] STN EN 31010.
[14] STN EN 31010.

- Systematic team approaches or expert assessments – where a team of experts follows a systematic process to identify risks using a structured set of challenges or questions.
- Inductive reasoning techniques – possible future expected events that can negatively affect the actor's intentions are analysed. They help to evaluate the probability of occurrence of events and their consequences, probability models are usually used that work with risk as a purely probabilistic quantity. This approach is based on the fact that the given phenomenon occurs with a certain probability, which can be determined on the basis of certain statistical variables (e.g. the number of occurrences of a given group of phenomena, the length of the monitored period, etc.). Since there can be a significant number of factors to be monitored, the process is often complicated and is only possible with the use of computer technology.

The output of the risk identification process is a verbal description of the risks in the list of risks that the actor undertakes. This is sometimes called the Risk Register, the Risk Catalogue, or the Checklist Risks. The risk description is an organised notation of the risk, which usually contains the elements shown in Figure 1.

List of risks			
Sources	**Events**	**Causes**	**Consequences**

Figure 1: The elements of the List of Risks
Source: Compiled by the authors

Risk analysis

Risk analysis refers to the development and understanding of risk. It is a process that involves understanding the nature of the risk and determining its level. It provides input into risk assessment and decisions about whether risks need to be modified and which modification strategies and methods are most appropriate. It can also provide input into decision-making where choices have to be made and the options contain different types and levels of risk. The risk analysis includes considerations of:[15]

[15] STN EN 31010.

- causes and sources of risk
- negative consequences of the event such as harm or damage
- the probability that these consequences may occur
- factors that affect the consequences and their probability, which can be an event that has multiple consequences and can affect different goals, or existing risk modification measures (risk management elements) that should be taken into account

The risk is analysed by determining:[16]

- consequences of the event
- probability of occurrence of the event
- other risk characteristics

The consequences and their probabilities are then combined to determine the level of risk. Risk analysis can be carried out with different levels of detail and depending on the risk itself, the purpose of the analysis, information, data and available resources. Analysis can be:[17]

- qualitative
- semi-quantitative
- quantitative, or
- depending on the circumstances, their combination

Qualitative methods use expert estimates, which are a direct expression of the occurrence of a risk event, determination of its size or significance, usually not directly supported by a formalised calculation. An expert estimate can be based on an intuitive assessment of the risk as a whole, i.e. without analysis of its individual quantities and assumptions, or a careful consideration of the qualitative importance of these quantities (risk parameters) and risk estimation as a quantity derived from these parameters. Expert estimates are mainly used in cases where numerical values (data) for quantitative risk assessment are missing or difficult to express, they are simpler and faster, but more subjective. Qualitative analysis is mainly used as an initial overview leading to the identification of risks that require more detailed investigation, where this type of analysis is sufficient for decision-making, or where numerical data or resources are insufficient to

[16] STN EN 31010.
[17] STN EN 31010.

perform a quantitative analysis.[18] It is advantageous to use qualitative inductive expert methods especially when solving risk analysis tasks in the field of physical security and facility security, because the conditions and prerequisites for the emergence of risks are very variable, the quantitative expression of risk parameters is very difficult due to the diversity of conditions and the significant influence of the human factor, qualitative methods do not require a lot of statistical data, but use logical links between factors influencing the emergence of risk, qualitative methods provide a clear and comprehensible description of risks and their parameters. Qualitative methods for risk analysis mainly use expert techniques: matrix of consequences and probabilities and the structure "What happens if?".[19] A verbal description is used to establish the level of importance, e.g. high, medium and low levels, but multiple levels can be used. A verbal description is more understandable and intuitively acceptable for most users. This procedure is relatively clear and simple, but there is a considerable degree of subjectivity in it, which uses subjective probability to describe individual events, expressing the degree of personal belief about the occurrence of the phenomenon (event) under consideration depending on the defined factors. Some authors assume that information obtained from qualitative analysis is almost always more valuable than from quantitative analysis, and then quantitative analysis is not always necessary. They recommend a qualitative analysis especially for the development of the initial risk assessment, which can later be refined with a quantitative analysis.[20] In semi-quantitative methods, numerical classification scales are used for consequence and probability and are combined to determine the level of risk using a formula. Scales can be:

- Linear – uniform division of the measurement range into a selected number of equal intervals with an abstract numerical value (0–X), or with a percentage value (0–100%).
- Logarithmic – the scale is the logarithm of a certain quantity, the increase of any value on the logarithmic scale by a fixed constant corresponds to the multiplication of the relevant quantity by a certain factor.
- Or they can express another relationship – the formulas used to determine the level of risk may also vary.

[18] STN EN 31010.
[19] STN EN 31010.
[20] STN EN 31010.

The goal is to create scales that are more detailed than qualitative analysis can usually provide. Numerical values replace the verbal expression of the size. In the numerical classification scale, it is possible to create more intervals or degrees than in the qualitative assessment. However, the goal is not to suggest realistic values for describing risks, as quantitative analysis attempts to do. Because of the numerical value assigned to each property may not represent an exact ratio to the actual magnitude of consequences or probability, these values should only appear in formulas that respect the constraints of established scales.[21] The semi-quantitative risk assessment procedure mainly uses the point method, in which numerical point values are assigned in the scales of probability and consequences, which are evaluated by a matrix. There are various formulas for determining the level of magnitude of a risk, but the most widely accepted formula for quantifying risk is:

$$R = P \times C$$

where R stands for the size of risk, P for the probability of event occurrence and C for the consequence of the event.[22] Special attention must be paid to the use of semi-quantitative analysis, because the numbers chosen may not correctly describe the reality, which may lead to inconsistencies or to unusual or incorrect results. Semi-quantitative analysis may not properly distinguish between risks, especially when the consequences or probabilities of events are extraordinary. In quantitative analyses, practical values for consequences and their probabilities are estimated and risk level values are determined in specific units, determined in the course of creating contexts. Full quantitative analysis may not always be possible or desirable due to lack of information about the system or activity being analysed, lack of data, influence of human factors, etc., or when quantitative analysis efforts are not warranted or required. Under these circumstances, a comparative semi-quantitative or qualitative risk classification, performed by experienced professionals in the relevant field, can still be effective. Even if a full quantitative analysis is performed, it can only be recognised that the calculated risk levels are also only estimates. It should be ensured that the level of accuracy and precision attributed to them is incompatible with the accuracy of the data and methods used. Quantitative methods use the numerical assessment

[21] STN EN 31010.

[22] Belan–Mišík 2016.

of risks by expressing their probability, frequency, credibility, potential, consequences, etc. These methods can be used primarily in cases where there is enough relevant data that can be evaluated statistically. They are mainly used in the field of information systems (they also include the vulnerability of the object). They mainly use statistical analysis (statistical characteristics of the degree of variability – variance, standard deviation, coefficient of variation), or simulation procedures (e.g. Monte Carlo, Markov analysis, Bayesian analysis). In some cases, a single numerical value is not enough to determine the consequences in different times, places or situations. The analysis should also consider and describe the uncertainty and variability of the consequences and their probability. These methods are more exact than qualitative, their implementation requires more time and effort, in some cases they can also be less clear, but they also provide a financial expression of risks, which is more advantageous for their management. To support the performance of quantitative risk analysis, special tools can be used in the form of software programs in which the methodology and system of risk analysis are already incorporated, especially CRAMM (CCTA Risk Analysis and Management Method), in the versions CRAMM expert, CRAMM express and BS 7799 (ISO 27001) Review. Also known are Decision Tools, Callio Secura 17799, COBRA, Counter Measures, EAR/PILAR, Ebios, Proteus and others.[23] The following methods are mainly used for risk analysis: HAZOP, Scenario Analysis, Root Cause Analysis, Event Tree Analysis, Cause–Effect Relationship Analysis, LOPA, Bow Tie Type Analysis, FN Curves, Risk Indices, Matrix of Consequences and Probabilities, CBA, MCDA, etc.[24]

Risk evaluation

The purpose of risk evaluation is to help in making decisions about risks requiring treatment and the priority of risks for the introduction of treatment. The risk evaluation includes:[25]

- comparison of the size of the risk detected in the analysis process, with the risk criteria determined during the creation of contexts
- consideration of the need for risk management

[23] Belan–Mišík 2016.
[24] STN EN 31010.
[25] ISO 31000.

- issuing a decision on risks that require treatment
- determining the priorities of these risks for the implementation of treatment

Decisions about risks that require treatment are based on the outputs of the risk analysis. The evaluation of risks is therefore intended to decide on the seriousness of risks for the actor, whether to accept a particular risk or to modify it with one of the ways of dealing with the risk. Risks are sorted according to their level of magnitude in categories such as acceptable, permissible or unacceptable, to determine whether it is worthwhile to modify the risk. Decisions should take into account the wider framework of risk and in some cases the risk assessment may lead to a decision to perform further analysis, or maintain the existing measures for managing it and not deal with the risk in any other way. Ethical, legal, financial and other issues, including risk perception, are used as inputs for decisions. Decisions should be taken in accordance with the requirements of laws, regulations and other requirements. The following aspects can lead to decisions:[26]

- whether the risk needs treatment
- priorities for treatment
- whether any activity is to be undertaken
- which of the many paths to take

The nature of the decisions that need to be made and the criteria that will be used to make those decisions have been decided during contextualisation, but at this stage, when more is known about the specific risks, more detail needs to be reassessed. Initial assumptions and results should be documented. The easiest way to define risk is a single level that divides risks into risks that:

- Require treatment – these include unacceptable risks and tolerable risks for which costs and benefits are assessed.
- Do not need it – acceptable level of risk.

This division gives temptingly simple results, but neither reflect the uncertainties included in risk assessment, nor define the boundary between risks that need treatment and those that do not. The decision about whether and how to deal with a risk can depend on costs and benefits, especially for tolerable risks when

[26] Belan–Mišík 2016.

taking a risk, or on the introduction of improved risk modification measures. A common way is to divide risks into three groups:[27]

- the upper group, where the level of risk is considered unacceptable, regardless of whether the activity can mean any benefit, and handling the risk is necessary at any cost
- middle group (or grey area), where both costs and benefits are taken into account, and opportunities are weighed against potential consequences
- the lower group, where the level of risk is considered negligible or so small that no measures to deal with the risk are necessary

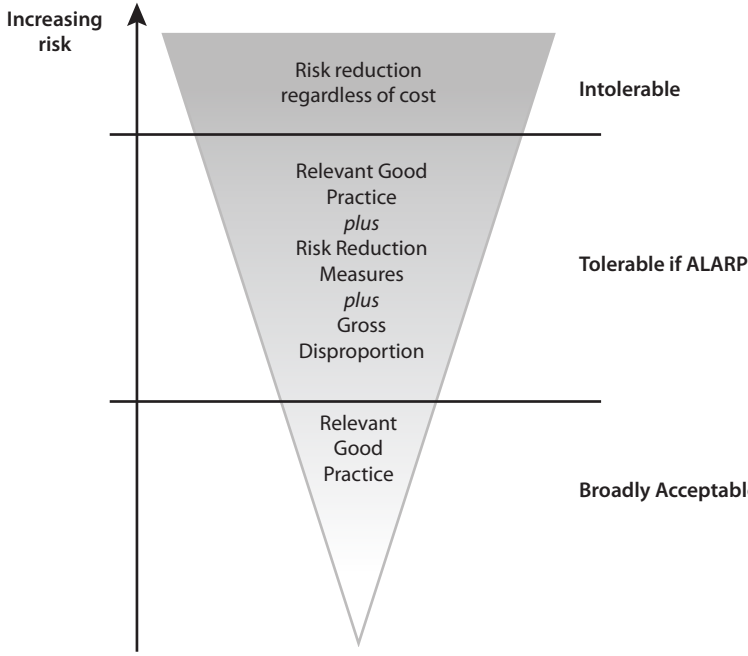

Figure 2: The ALARP principle
Source: www.shorturl.at/noPY6

[27] Belan–Mišík 2016.

To assess the costs and benefits of selected ways of dealing with unacceptable and tolerable risks, the ALARP principle ("as low as reasonably practicable") is used, which shows that appropriate attention should be paid to risk, risk management and risk modification. The principle involves weighing and comparing the level of risk with the difficulty, time and financial costs required to manage it. The ALARP principle is shown in Figure 2.

ALARP mainly addresses the middle group, where there is a sliding scale for tolerable low risks, for which costs and benefits can be directly compared, while for undesirable high risks, the possibility of damage must be reduced, unless the expenditure for further reduction is significantly disproportionate to the safety benefit obtained.[28] The result of the risk assessment should also be the compilation of the order of priority of the risks that require treatment. The ranking assigns a rating to each risk and thus sets priorities for dealing with risks. Risks requiring treatment will not always be able to be adjusted immediately, for a number of reasons, e.g.:

- time requirement
- material – technical difficulty
- financial difficulty
- high demands on human resources
- strategic intentions of the actor, etc.

The stated reasons also influence the priorities of the risks for the implementation of the chosen methods of dealing with them. The goal is to sort the assessed risks according to their significance or priority by using the selected criteria and procedures. It is the decision-making process that uses selected criteria to prioritise risks that require some treatment. The output of the risk assessment is a list of risks that require treatment according to treatment priorities. Based on the determined priorities, the order of risks is determined for the choice of method/methods of dealing with them.[29]

[28] Belan–Mišík 2016.
[29] Belan–Mišík 2016.

Table 1: The risk assessment content

Risk assessment		
Risk identification	**Risk analysis**	**Risk evaluation**
The process of finding, recognising and describing the risk	A process for understanding the nature, sources and causes of risks to assess the level of risk	The process of comparing the results of the risk analysis with the risk criteria
It includes an identification	It includes an assessment	It includes an evaluation
– **sources** of risk – elements that by themselves or in combination have the internal potential to cause risk and the areas of their consequences – **events** that risk sources can cause – **circumstances** that could have potential consequences for achieving goals – **causes of risk** – *what* can happen, *when* and *where, why* and *how* it can happen – potential **consequences** – **measures** introduced to modify the risk	– **causes and sources** of risk – danger (threat) – **negative consequences** of the event – loss – the **probability** that these consequences may occur – **other characteristics** of the risk – factors that influence consequences and probability	– **comparison** of the level of risk from the analysis process, with the risk criteria determined during the search for connections – **consideration of the need for risk treatment** – issuing a **decision on risks that require treatment** and determining their priorities for treatment
List of risks	List of **hazardous events** – documented sources of risk and factors that affect consequences and probability **Level of risks**	**Deciding on risks that require treatment and prioritising them for modification**

Source: Compiled by the authors

Conclusion

Hybrid threats have their own characteristics, therefore assessing the risks, the source of which is at the heart of a hybrid threat is a difficult process. These are relatively new, serious risks that significantly affect the safety of people, property and the environment. A security actor existing in an uncertain, ever-changing

environment must have the ability to adapt or change in order to achieve a certain consistency of his own activity, his own goals with environmental conditions that change and which can be a source of instability with all its effects on individual factors broader and immediate external environment. Risk management is therefore one of the most important issues facing actors today. It is an important part of any strategic management. There are several procedures, in this work we focused on the ISO 31000 process.

Questions

1. Define risk and security risk, and list possible sources of risk.
2. State the content of the risk assessment, and describe the principles of risk identification.
3. Characterise risk identification methods, and risk analysis methods.

References

Belan, Ľubomír – Mišík, Ján (2016): *Manažérstvo bezpečnostného rizika* [Security Risk Management]. Žilina: Žilinská univerzita.

European Commission (2016): *Common Framework for Combating Hybrid Threats.* Joint Communication to the European Parliament and the Council. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

Hofreiter, Ladislav (2015): *Manažment ochrany objektov.* Žilina: Žilinská univerzita.

IEC 31010:2019: Risk Management – Risk Assessment Techniques.

ISO 31000:2018: Risk Management – Guidelines.

ISO/TR 31004:2013: Risk Management – Guidance for the Implementation of ISO 31000.

IWA 31:2020: Risk Management – Guidelines on Using ISO 31000 in Management Systems.

Jurčák, Vojtech – Kredatus, Ondrej – Ivančík, Radoslav – Ganoczy, Štefan – Pikner, Ivo – Jurčák, Ján – Sasarák, Jakub (2017): *Identifikácia príznakov vedenia hybridnej vojny* [Identifying the Signs of Hybrid Warfare]. Záverečná správa oriešení vedeckého projektu VV-A1 [Final Report of Research Project VV-A1]. Liptovský Mikuláš: Akadémia ozbrojených síl generála Milana Rastislava Štefánika.

Laml, Roman (2008): *Vzťah pojmov hrozba a riziko (II).* Online: http://mepoforum.sk/bezpecnost/terminologia/vztah-pojmov-hrozba-a-riziko-ii-roman-laml/