Zsolt Pastorek – Matúš Grega[1]

Bases for Simulating Hybrid Threats

Crisis scenario

Crisis scenarios describe development variants – a past event as a generalised experience or a description of a possible or probable crisis. Due to the unrepeatability of crises on the one hand and the need to learn lessons for the future, crisis scenarios work with an acceptable level of uncertainty of the course of the crisis and alternatives to its course as well as future post-crisis development. This approach corresponds to the degree of knowledge of the security environment and its variability in development in the short, medium and long-term future. Crisis scenarios can be defined as a generalisation of expertise from the development and course of unique events that have a destructive and negative impact on human life, society and social infrastructure, their accepted values, conditions and prerequisites for valuable, prosperous, prospective sustainable development and safe life in the form of elaborated topics. Crisis scenarios mediate the progress and chaining of isolated and interconnected essential processes and events in time and space dimensions. Based on their depth and degree of scientific knowledge, crisis scenarios are also part of security theory, the security policy of states, and tactical as well as strategic planning. Crisis scenarios also become part of the system of training crisis managers as an essential tool for expanding their competencies and abilities to solve specific crises and increasing their readiness to solve possible variants of crisis situations in the future. It is precisely for these purposes that typical crisis scenarios are developed, which are a generalisation of knowledge of the primary phases of crisis development to a specific type of threat, e.g. fire, flood, war conflict, hybrid threats, with an appropriate degree of abstraction from the concrete and unique. Type crisis scenarios further define the primary groups of activities of the aid and rescue management entities, as well as forces and means to minimise the negative impact of activated destructive forces and

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

DOI: https://doi.org/10.36250/01238_06

processes. They make it possible to know the individual type of threat in a given security environment, point out the basic variants of the development of a crisis, and present a basic model of the activities of the management and executive forces of rescue and counter-reaction to crisis processes. Typical crisis scenarios have a fixed structure according to the mission of a specific type of scenario. We can consider the following model as the standard structure of a crisis scenario:

- source of threat, circumstances and cause of the crisis, harmful and destructive effects – consequences, standard spatial and temporal course and stages of development of the crisis
- reaction and measures of parts of the security system – crisis management to the emergence and increase of threats to parts of the social system from the crisis in question; measures and activities until the end of the crisis and threat, basic measures for restoration, reconstruction and minimisation of the recurrence of the situation – risk
- activity of affected and threatened systems and persons in all stages of the crisis

Design of the structure of a typical scenario for a hybrid threat

In creating crisis scenarios of hybrid threats, attention was and is mainly devoted to identifying decisive – main risks and factors that activate hybrid threats and potential threats and release unexpected adverse events, energies, substances and processes. In crisis scenarios, descriptions of possible variants of development in linear or branched procedures are developed with an emphasis on their relevance, science and reality. An essential factor for creating hybrid threat crisis scenarios is also the *target audience* (trainees) and the goals for which the simulation will be carried out. In this context, from the point of view of the selection of scenarios, the trainees can be divided into the following groups:

- high school and university students
- workers in the state administration, personnel in local government
- military personnel

Each of the mentioned groups has defined different goals:

- *High school and university students:* The goal is to learn about the nature of hybrid threats and possible ways to combat such threats. The primary goal is to point out the complexity of hybrid threats and their potential impact on the real development of the situation.

- *Employees in the state administration:* For the mentioned audience, the exercise scenario must focus on forms of hybrid threats and ways to fight against them. The scenario should support knowledge regarding how individual state institutions are connected and their role in eliminating hybrid threats. The set scenario should also fully evoke critical thinking in the trainees.
- *Military personnel:* The focus of the exercise should reflect the needs and specifics of Military–Civilian Cooperation (CIMIC) and involve hybrid warfare in the Military Decision-Making Process (MDMP). To develop practical skills for early recognition of the hybrid conduct of an armed conflict, to develop the communication skills of military personnel towards the public, and to prepare military professionals for the risks arising from hybrid threats at the time of a war operation.

A precise definition of the *exercise level* is necessary when creating an exercise framework. The level of the trainees, the geographical area and the complexity of the subject are defined. For this approach, performing a horizontal, vertical and geographical division of hybrid threats is appropriate. The horizontal division is based on the designation of irregular–unconventional methods used alongside conventional warfare. As part of the horizontal division of the hybrid attack, we can count on the topic exercises with phenomena such as fake news, criminal and terrorist activities, etc. Before creating crisis scenarios for practising hybrid threats, it is also necessary to define the vertical level of the practised issue. This consists of the definition of the operative level of the exercise scene. It can be strategic (at the level of states, nations), tactical (larger territorial units, communities) or operational (at the level of local government, purpose-built groups operating in a small area). The last necessary variable for the definition of any simulation exercise is the geographical space and its division where the exercise in question will take place. The process of creating crisis scenarios for practising hybrid threats includes the following stages:

- Determining the content and goal of the crisis scenario for the target audience, the so-called scenario framework. Defining the scenario framework includes defining the central plot situation, the so-called topic, the goal, why we are solving the given case and what we want to achieve with the results. The practical impact of hybrid threats manifests itself, especially during events that negatively expose society. In such cases, hybrid action acts as a catalyst for the primary problem and causes more damage. In terms of content, it is, therefore, appropriate to choose a scenario where the primary issue will be solved – a "standard crisis". Solving the mentioned problem will be complicated by the hybrid effect on individual aspects of the situation. In case of the civil sector, it will mainly be about maintaining the effectiveness of the rescue system. In case of military personnel, the goal will be to fulfil a combat mission. In the content of the scenario defined in this way, the goal will be to minimise damage by eliminating hybrid threats and maintaining an effective system of rescue and security services or maintaining the dynamics of the military operation.

- Delineation of decisive facts, events, processes and factors, and determination of their importance and interconnectedness is the basic framework of the crisis scenario. Determining the content is based on experience, practical needs and analysis of the security environment, as well as current and future security threats and challenges. The mission of the crisis scenario is expressed and concretised in its goal and answers the question of why we are solving a specific scenario, what do we want to investigate, how large is the number of variables, what are their dynamic relationships, how to integrate them into an understandable plot unit, what are the optimal outputs for the needs of the crisis management.
- Defining the decisive dimensions and limits of the crisis scenario. The reality and scientific nature of the incorporated and accepted limits are conditions for usability and practical and theoretical contribution because they specify the content and create prerequisites for fulfilling the goal of the crisis scenario. We consider the decisive limits and dimensions of the crisis scenario to be:
    - quantitative and qualitative characteristics of the crisis in the destructive, temporal and spatial dimensions – the dimension of the crisis situation (phenomenon)
    - characteristics of the security environment, relations between the environment and the crisis – definition of the positive and negative dimensions of the environment and the crisis
    - interested subjects – forces and means of crisis management, affected and disabled actors (persons, animals, technical system, etc.), their limits (possibility, capabilities, etc.) and activities

  - a group of additional information and characteristics specifying, in a linear and a branched variant, the dimension of the crisis to ensure the consistency of its dimensions
- The process of creating a starting variant and crisis scenario model. Based on the above mentioned requirements and starting points, a group of experts has developed a starting variant of the crisis scenario that best reflects the client's starting requirements.
- Correction of the draft crisis scenario. Based on the analysis of the starting points, the goal and the content of the crisis scenario, the possibility of practical or theoretical use of the scenario is evaluated in the form of an expert or specialist assessment according to its type and purpose. Attention is focused, for example, on the scope of incorporated information, available supporting documents, the time of crisis scenario solvers to complete tasks, etc. Emphasis is placed on the usefulness, practical or theoretical significance of the crisis scenario, e.g. for the needs of crisis management of public administration at the local level, it should mainly deal with the issue of threat sources based on the analyses of specific territory for the needs of civil protection, in case of the armed forces, e.g. the issue hybrid threats that activate a war conflict or a crisis situation of a military nature with the deployment of armed forces. The scenario is modified, supplemented and optimised according to the established requirements for individual groups of crises.
- Verify the correctness and validity of the draft crisis scenario. According to the type and nature of the crisis scenario, the optimal method of its verification is selected, which usually takes the form of a practical verification, e.g. a practical experiment, an exercise, a theoretical proof, e.g. a theoretical model, a mathematical model, or a combined form, e.g. a practical training with a simulated process of the unexpected negative phenomena and events. After a theoretical or practical verification of the correctness of the applied model of the crisis scenario, positive and negative findings are incorporated to an adequate extent according to their significance into the crisis scenario and related documents – plans, methodological guidelines, activity methodologies and the like.
- Include and place the crisis scenario in the existing portfolio (catalogue of typical crisis scenarios, catalogue of specific crisis scenarios). The state and development of the security environment require selecting topics and

developing several crisis scenarios, which cover all anticipated crises and their variants. Newly developed crisis scenarios for hybrid threats must respond to new processes and events, forces and means, be representative, and cover key characteristics of current and anticipated crisis situations. The portfolio of crisis scenarios should cover the entire spectrum of crises, create and present links between individual scenarios and security reality, replace outdated and unrepresentative scenarios with new ones, and thus respond to the dynamics of risks and crises.

Exercise level

The exercise level primarily defines the scenario itself. However, it is also necessary to emphasise the connection with the required technical equipment. Up to the operational stage, when, in addition to team cooperation, the individual capabilities of individuals are also practised, it is possible to use the means for virtual reality fully. With a more significant number of trainees, virtual reality loses its justification, and it is necessary to bring the means of constructive simulation to the fore. Thanks to the aggregation of entities, the latter can very effectively imitate hybrid threats and their impact on target groups. In case of a requirement for a simulation exercise for the security community, the starting points are as follows:

- the range of practised hybrid threats (horizontal division) is limited to:
  - fake news, influencing public opinion through social networks and inciting civil disobedience during a standard crisis – leakage of a dangerous substance
  - cyber threats (attacks) such as password pawning, phishing and security breaches via the USB port
- within the vertical division, the exercise scene is at the operational level of the municipality and the crisis staff
- the geographical space is defined by the area of two municipalities with a population of 1,500 and a base map area of 32 × 15 km

The crisis scenario is chosen to acquire theoretical and practical skills in "combating" hybrid threats in times of crisis. The scenario makes it possible to change the difficulty of the situation, enabling a simulation exercise both for students in the field of crisis management and for members of the crisis staff of municipalities and various state agencies. The following three chapters describe two scenario types. The first scenario type is set in a *civilian environment,* where the crisis defines the problem, and the staff has stressor factors in solving the problem: time and hybrid threats. The consequence of these threats is the disobedience of citizens in the evacuation process. The second scenario type is set in a *military environment* and employs blended tactics by all operational audiences. Within it, the manifestation of hybrid attacks results from the judicious combination of conventional, unconventional and asymmetrical tactics, techniques and procedures (TTP) launched by regular forces and irregular elements.

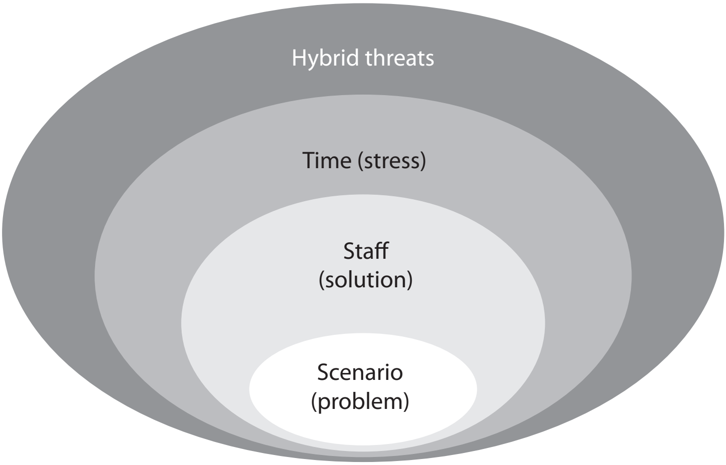

Figure 1: Basic principle of hybrid threat simulation
Source: Compiled by the authors

Conclusion

Considering the mentioned starting parameters, the scenarios prepared for the exercise to support education and prepare the security community for solving the tasks of eliminating hybrid threats should have the following structure:

- general description before the emergence of a crisis
- identification and characteristics of simulated entities
- requirements for visualisation of the external environment
- requirements for visualising the interior spaces of selected objects
- characteristics of the crisis and characteristics of hybrid threats
- specification of the numbers and type of forces and resources used
- anticipated activity of citizens and self-government bodies
- anticipated activity of state administration bodies, special teams and components of the integrated rescue system
- stabilisation phase and post-conflict situation