Anna Rolka

2. CRISIS MANAGEMENT

Citizen safety is one of the main responsibilities of the State. State authorities should be prepared to protect people and critical infrastructure at all times, especially during disasters, accidents, or terrorist situations.

2.1. Basics of crisis management

2.1.1. The essence of crisis management

A crisis situation is a situation adversely affecting the level of safety and security of people, property and the environment, and causing significant restrictions on the operation of public authorities, if they are inadequately prepared and lacking capabilities and resources.

In crisis management, some of the work of the authorities can touch on elements of national security, but mainly consists in preventing crisis situations, preparing to assume control of crises through planned actions, reacting to crisis situations, restoring order and repairing the original character of the public infrastructure, as necessary.

Crisis management is understood as a complex of the activities taken by the competent authorities to control the crisis, as well in developing preventative measures. This involves several key principles:

– The principle of primacy of the territorial authorities – decisions should be made at the lowest level of the administrative division in the affected area;

– Single-person decision-making and responsibility – decisions (commands) should be made by a person at a high level of local government in the affected area;

– The principle of adequacy – the authorities at the lowest level of administration in the affected area should be competent first-responders;

– The principle of universality – all of the citizens in the affected area should be prepared to help the authorities deal with the crisis, with their local authorities able to ask everybody to help (through administrative decisions, decrees, etc).

2.1.2. Crisis management cycle

Activities in crisis management should be made as effective as possible. Proactively, public authorities should not wait until a crisis situation occurs – it is very important to reduce the probability of occurrence of threats and to reduce the potential effects. One of the most important attributes of crisis management is its division into four phases – Prevention, Preparedness, Response and Recovery. In the holistic view, these phases involve whole actions leading to elimination of threats, recovery from the threat, and development of the awareness and preparedness of citizens for further threats.

The objective of the **first phase** (Fig. 1) is to focus on preventing incidents before they happen. It is very important to be able to determine the symptoms of trouble, and thus initiate an appropriate response. This phase involves people who can identify danger, assess its risk and advance a response plan. This is the time for improving environmental protection, especially through local government policy. In this phase, the authorities can build people's knowledge of threats and raise awareness in local communities through public education.

The prevention phase includes:
1. Identification of threats;
2. Searching for the source of threats and recognition of risks;
3. A process of describing risks;
4. Analysis of the previous response phase and answering questions about it;
5. Analysis of the previous recovery phase;
6. Analysis of planning documents – making necessary changes as a result of the response and recovery phases;
7. Updating lists of threats – making necessary changes as a result of the response and recovery phases;
8. Updating of databases (addresses, materials, medical information, fuel etc);
9. Development of new educational programs.

Threat identification requires data to be collected and analysed. This can be done through:
– Analysis of statistical data;
– Analysis of historical data;
– Expert assessments;
– Field studies;
– Assessment of the international situation;
– Mathematical modelling;
– Analysis of data from threat monitoring systems;
– Analysis of trends;
– Examination of historical cases (case studies, 'lessons learned' etc.);
– Environmental diagnosis, etc.
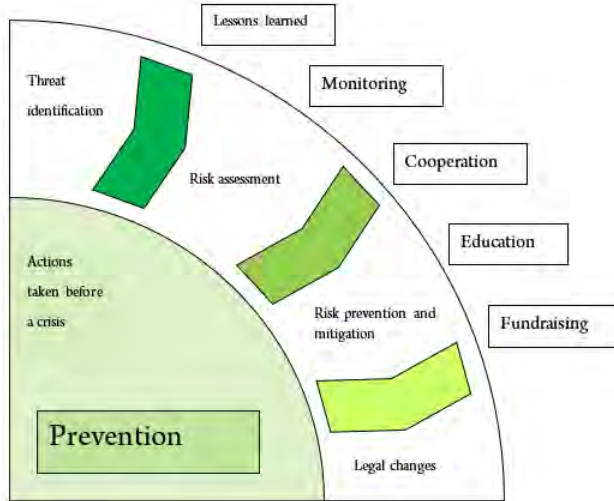
Figure 1. The first phase – Prevention

The process of determining sources of threats and recognizing risks is the first step in risk assessment. Threats can develop in several different ways, depending on, for example: the speed of the emergency services' response; the type of weapon used and the method of its release; the time, location and weather, and the preparedness of the authorities (their coordination, management and level of support, etc). Consequently, it is necessary to specify almost all of these factors in the prevention phase.

In terms of deciding whether a risk is acceptable or not, there are four categories:

A – **Acceptable**: no additional security measures are required; the current solutions and their assigned capabilities and resources, as well as their monitoring processes, are all strong.

T – **Tolerable risk (permitted)**: alternatives must be considered, whether they be the introduction of small changes, legal or functional, and whether or not they will improve safety or the public's feeling of safety.

ToC – **Tolerable on Condition**: additional security measures should be introduced within the next six months, and existing solutions should be improved.

U – **Unacceptable**: immediate action should be taken to enhance security, and new solutions should be introduced.

Bear in mind that there are two possible areas of risk: risks resulting from actions taken directly by a person, and risks resulting from processes occurring in the human environmen. This is particularly important when analysing risks from the point of view of CBRN incidents.

The concept of 'Lesson learned', which we refer to in this text, should be understood as an activity or methodology based on experience gained from evaluating projects, programmes and policies that are abstracted from specific circumstances to broader, more generalised situations. Frequently, the process of determining what lessons have been learned from experience can highlight strengths and weaknesses in preparation, design, and implementation that then affect performance, and the outcome and impact of future incidents.

Finally, it is important to note that there is no gap between the first phase (Prevention), and the second phase (Preparation).

Exercise 1

Working in groups of four, think about CBRN threats. Choose one and discuss:

1. Have any lessons be learned about this type of threat in your country?
2. What can we do to prevent or mitigate the risks posed by this threat?
3. Present the results and conclusions of your group discussion.
4. Are these conclusions positive, or not?

The **second phase** is the preparation phase (Fig. 2), and is dedicated to planning for incidents. The most important goal here is to prepare people and resources properly for direct use in the next (third) phase. All activities are focused on arranging and developing crisis management plans and improving the different documents needed to properly respond to diagnosed threats. In this phase, the authorities are focused on minimising potential damage or increasing public endurance to terrorist threats. It is the likelihood of the occurrence of threats and incidents is the centre of attention here.
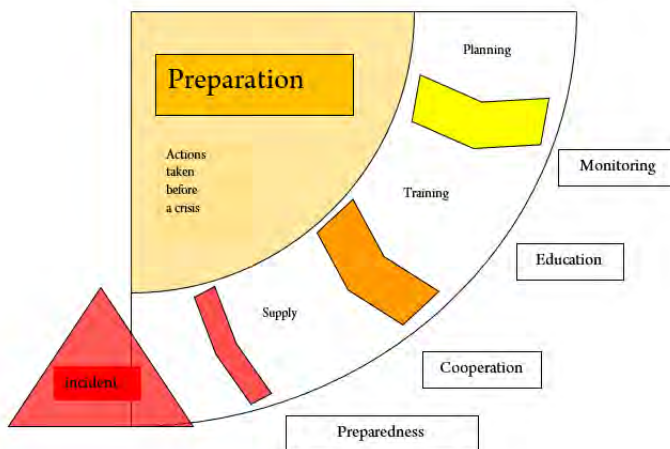
Figure 2. The second phase – Preparation

The principal parts of the preparation phase are:

1. Planning;
2. Preparation and implementation of response procedures;
3. Training of personnel in best procedures for dealing with threats;
4. Preparation of communication systems;
5. Preparation of logistics support, its assessment and supplementation (if required).

Some of the tasks involved are common to both the prevention and preparation phases. For example:

1. Continuous monitoring of sources of threats, and recognition of risks;
2. Educational activities by local authorities, NGOs, rescue services etc.;
3. Development of the cooperation between local authorities, state agencies, emergency services, NGOs etc.

Part of the preparation phase involves assigning responsibilities to various institutions and authorities in the event of an incident. There are three categories of participant, in terms of assigned responsibility:

– Leading institution (L) – The institution or authority tasked with preventing and combating threats. This is usually an executive authority in terms of actually reducing the level of risk and responding to the threat. There is only one Lead.

– Coordinating institution (C) – The institution or authority whose task is to coordinate (when needed) the activities of support and rescue entities involved in responding to crisis situations.

– Auxiliary institutions (A) – The institutions or authorities involved in the efforts to reduce the level of risk and respond to the threat.

The result of all of this analysis and preparation will be a set of tasks for, and responsibilities assigned to, the various participants involved in crisis management. This will take the form of a 'security matrix' (Table 1).

Table 1. Part of a security matrix

| No.	CM Participant	Radiation	Infectious diseases	Hurricanes	…
1	Voivode	L	L	L	
2	Fire Service	A	A	A	
3	Police	A	A	A	
4	Ambulance Service	A	A	A	

A correctly prepared security matrix allows for determination of synergies between crisis management participants – whether a given institution or authority will, in a given scenario, fight a threat on its own or together with another authority or institution.

The **third phase** of crisis management is the response phase (Fig. 3). This begins when an incident occurs, and continues throughout it until the crisis/threat has been nullified. The goal of all actions taken in the response phase is saving the lives and health of people, property and the environment (including rendering aid to the injured and trapped). It is also very important to minimise economic damage and stop subsequent crime (theft, looting, public disorder, rioting etc.).

The practical work of the response phase lies in defining the priorities for responding to the threat, and to finding ways of minimising their impact. Existing CM plans and responses are put into action. The response phase includes:

1. Coordination of rescue and security measures;
2. Activation of necessary procedures and security entities;
3. Monitoring of current and subsequent threats and their consequences;
4. Implementation of decisions on the use of forces and means, with potential revision of plans for their use;
5. Coordination of the activities of the involved institutions and authorities;
6. Coordination of security and rescue services;
7. Coordination of the logistical protection of people affected;
8. Opening of information points for the population;
9. Introduction of necessary legal solutions.

Ultimately, the nature of the tasks carried out in the response phase is directly determined by the nature of the crisis, the extent of its effects and damage.
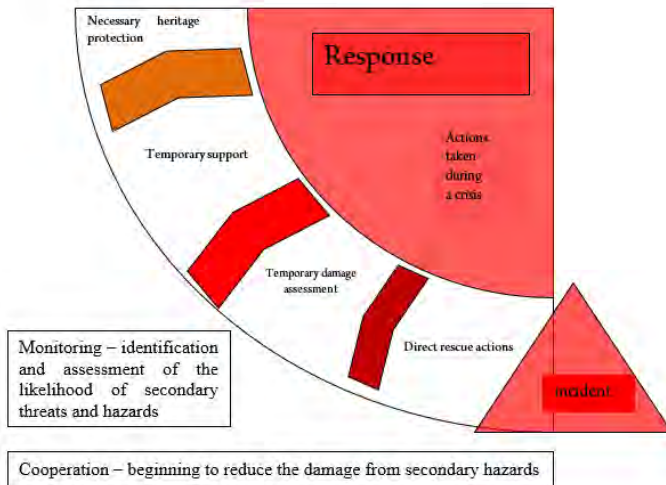
Figure 3. The third phase – Response

The **fourth phase** is the recovery phase (Fig. 4). The recovery phase begins when the activities of the response phase – to rescue and protect people, property

and the environment during a crisis – have run their course. Due to the nature of a crisis situation and its effects, this phase can have the longest duration. It can even overlap with the phases of prevention and preparation in the new crisis management cycle.
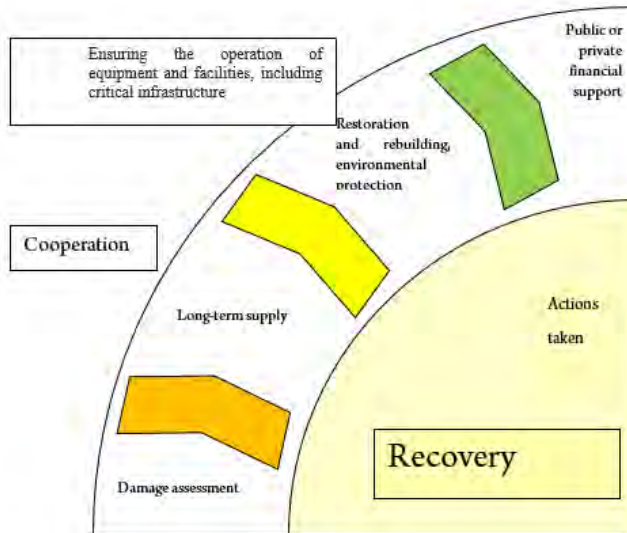
Figure 4. The fourth phase – Recovery

The most important tasks in the recovery phase are:
1. Damage assessment;
2. Running individual and collective aid programs for the affected populace;
3. Mobilizing financial assistance;
4. Ensuring the proper functioning of infrastructure, especially critical infrastructure.

Reconstruction after a crisis event is also an opportunity to correct previously made mistakes ('lessons learned'). It also allows for legislative work to improve security in the future.

2.1.3. Planning

In crisis management planning, the goal is always to secure the safety of the citizenry. The popular notion is that a CM plan is a list of definitive actions that should be taken in various crisis situations. But crisis management is a never-ending process, and so planning for crisis situations also never ends. A good CM plan should not be an all-encompassing document, as this creates false senses of security and preparedness. Additionally, it is not possible to anticipate every

threat. In fact, as soon as a CM plan is written, it begins losing its effectiveness. Furthermore, when the authorities need to implement their CM plan, they will find their options restricted from the outset – a CM plan can also be a barrier to flexibility.
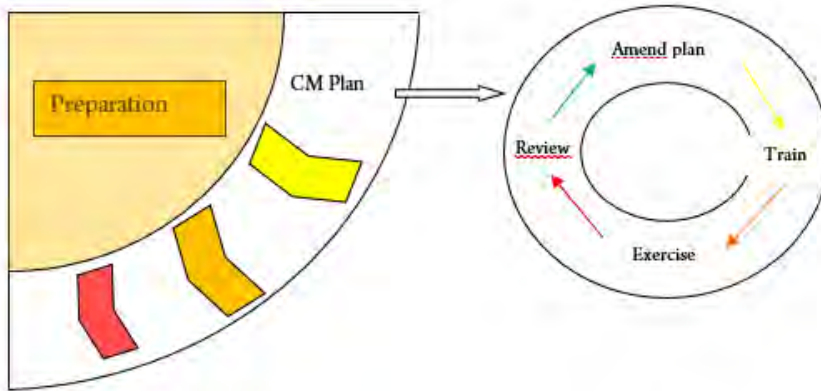
Figure 5. The preparation phase with the CM planning cycle

To begin thinking about a good plan, several important questions must be asked:
1. Why are making a CM plan?
2. Who or what necessitates having a CM plan?
3. Who is going to create the CM plan?
4. What has to go into it?
5. Do we need to test the plan?
And so on.

Effective crisis management planning is based on six activities:

1. Anticipation – What are the risks and threats out there? What new threats and hazards could arise? Having identified them, their potential impact must be assessed in order to effectively inform the level of planning needed to mitigate or eliminate them;

2. Assessment – Quantifying and analysing these threats by risk. A well-conducted risk analysis avoids the phenomenon of 'over-planning' which can paralyzed or choke the action when it needs to be taken;

3. Prevention – how to reduce the risk or prevent the incident from happening;

4. Preparation – training and exercises;

5. Response;

6. Recovery – return to normality.

CM plans need to satisfy a number of criteria:
1. There must be clear ownership of the plan;
2. The plan's actual, physical layout must be clear and easy to read;
3. The plan must be concise and to the point;
4. Roles and responsibilities must be clearly defined;
5. The plan must be revised and tested regularly;
6. All participants in the plan must be trained and regularly briefed.

A CM plan should have three parts:
1. The main plan, which lists:
   a) A description of likely threats and a risk assessment of their occurrence in your country (including threats to critical infrastructure), with risk maps and a map of potential threat locations,
   b) The responsibilities of the participants in crisis management procedures, in the form of a security matrix,
   c) The capabilities and resources marked for use in crises.
2. A description of how to proceed in crisis situations:
   a) Tasks related to threat monitoring,
   b) Procedures for activating the necessary capabilities and resources marked for use in crisis situations,
   c) Procedures for emergency responses, descriptions of what to do in crisis situations.
3. Functional annexes:
   a) Procedures for initiating necessary in a crisis management situation,
   b) Organisation of communications,
   c) Organisation of threat monitoring, warning and alarm systems,
   d) Rules for informing the population about threats and procedures in case of a crisis,
   e) Procedures for evacuating endangered areas (this can also be a separate plan),
   f) Rescue, medical care, and post-crisis social and psychological support procedures,
   g) Procedures for protection against area-specific threats,
   h) A list of all necessary signed contracts and agreements.

Exercise 2

Draw a 'bow-tie' diagram (as shown below) to visualise risk management and communicate the context of the controls in place, in your country. Identify the causes and potential consequences of a crisis situation (for example, CBRN). Try to identify what could help prevent dangerous situations from getting out of hand, and identify the indicators that will help to track potential changes.
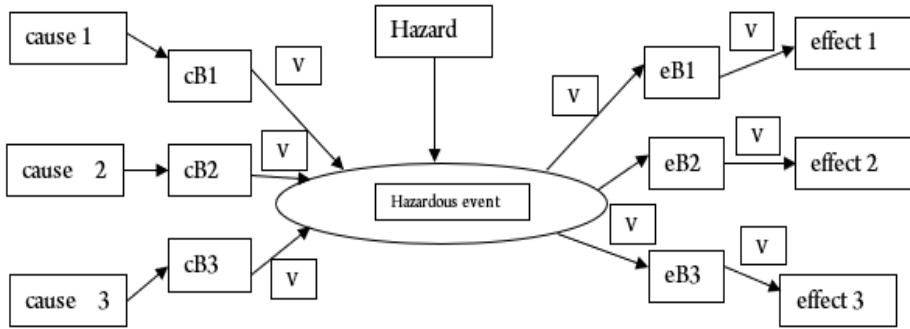
Figure 6. Bow-tie diagram: B – barrier; c – cause; e – effect; V – variable
(control indicator)

Exercise 3

Based on exercise 2, discuss the causes of threats/hazards. Include people (crisis participants), places, times, authorities, emergency services, etc. Think about the variables behind the causes, such as the emergency services, their equipment, training, responsibilities etc…. (up to 5 items per variable). Then, using the identified items and variables, create a table like this:

Causes /variables	Small problem ☺	Middling problem ☹	Big problem ☠
Services: – Equipment – Training – Command			

As you can see, crisis management plans form the basis for the response of the various authorities and institutions involved in securing the safety of citizens in a crisis. And as discussed earlier, in the section on the fourth phase of crisis management, CM plans identify the key institutions and authorities involved in crisis response. These are categorised in one of three ways:

– **Leading institution (L)** – The institution or authority tasked with preventing and combating threats. This is usually an executive authority in terms of actually reducing the level of risk and responding to the threat. There is only one Lead.

– **Coordinating institution (C)** – The institution or authority whose task is to coordinate (when needed) the activities of support and rescue entities involved in responding to crisis situations.

– **Auxiliary institutions (A)** – The institutions or authorities involved in the efforts to reduce the level of risk and respond to the threat.

Exercise 4

Working in groups of three, think about the institutions and authorities in your own countries. Which of them would be Leading, Coordinating or Auxiliary in a given crisis situation? Make a list of your answers and compare it with your colleagues'. Are there any differences? If so, why?

2.2. Crisis management system

The safety of a nation's citizens is the main purpose and responsibility of the State. Protection of the citizenry is achieved through defence of the population and critical infrastructure during times of crisis, disaster, large-scale destruction or other extreme incidents.

National and civil protection systems are part of a state's national security infrastructure. Part of this is a crisis management system (CMS), which is a system for handling emergency responses, controlling them by means of pre-planned actions, responding to the occurrence of threats and, later, restoring comprised infrastructure and resources. A CMS is designed to cover both emergencies and long-term operations. It integrates information with decision-making processes and a set of necessary security matrices. The purpose of a CMS is to neutralise or eliminate crises and threats.

When comparing the crisis management systems of different countries, it is almost impossible to find two very similar. Every country has its own CMS, tailored to its own unique needs and abilities. However, beyond the specific there are some components of a CMS that are common to all nations:

At the top level of planning for the protection of people and infrastructure, common elements include:

1. Population protection systems as part of the national security infrastructure;

2. Unified systems of observation, early warning, announcement and management in crisis situations, with integration with other security forces;

3. Principles of resource management to mitigate weaknesses and improve reactions and post-crisis restoration processes;

4. Public Private Partnerships;

5. Use of civil organisations;

6. Effective international partnerships;

7. Use of the most effective combination of regular and voluntary groups.

At the national government level, common elements include:

1. Formulation and conduct of a national policy on common leadership in crisis management;

2. Development of risk evaluation procedures;

3. Definition of the legal persons and firms assigned roles in planning, preparing and carrying out activities for/in a crisis;

4. Signing international and bilateral agreements on information sharing, assistance and mutual cooperation;

5. Coordination of educational activities and training exercises, scientific research and technical developments related to the crisis management system;

6. Implementation of a national crisis information system.

At the Crisis Management centres' level, common elements include:

1. Twenty-four hour oversight of the flow of information for crisis management needs;

2. Preventive control – a complex of measures ranging from analysis and classification of risk, to development and implementation of programmes and measures preventing and mitigating the consequences of crises on health and life, nature and the national economy;

3. Response coordination – the fundamental purpose of a CM centre;

4. Flexible planning that is often actualised immediately;

5. Monitoring of potential threats and analysis and evaluation of threats and their development;

6. Warning;

7. Oversight;

8. Cooperation with various NATO and EU units, and other international organisations and authorities;

9. Conduct of training and exercises in crisis management, with participation in national and international field exercises.

At the regional government level (the middle tier of crisis management), common elements include:

1. Coordination and leadership of crisis management in the region;

2. Organisation and oversight of crisis management plans in the region;

3. Coordination of crisis management tasks between regional organisations/ authorities;

4. Responsibility for maintaining crisis management systems;

5. Preparation and implementation of information and warning systems.

At the street/community level (the lowest level of crisis management), common elements include:

1. Organisation and implementation of crisis management in the community;

2. Preparation of evacuation/safety plans;

3. Organisation and implementation of rescue teams, and fund-raising for the prevention and mitigation of crises;

4. Organisation and implementation of the evacuation of local residents etc.

As an example of a European system, Figure 8 below shows the Polish Crisis Management System.

```
┌──────────────────┐   ┌──────────────────────┐   ┌──────────────────┐
│  The Minister    │◄──│ The Council of       │   │  Other Ministers │
│ of Internal      │   │ Ministers            │   │                  │
│ Affairs          │   │                      │   │                  │
└──────────────────┘   └──────────────────────┘   └──────────────────┘

        ┌──────────────────────┐   ┌──────────────────────┐   ┌──────────────┐
        │ Government Center    │   │ The Government Crisis│   │ Ministry CMC │
        │ for Security (RCB)   │   │ Management Team      │   │              │
        └──────────────────────┘   └──────────────────────┘   └──────────────┘

┌─────────────┐
│ National gov.│
└─────────────┘
```

```
┌──────────────────┐   ┌──────────────────┐   ┌──────────────────────────┐
│ Combined         │   │  The Voivode     │──►│ Experts, Voivode Marshal,│
│ voivodeship      │   │                  │   │ un-combined voivodeship  │
│ services,        │   │                  │   │ services                 │
│ inspectors and   │   └──────────────────┘   └──────────────────────────┘
│ guards,          │   ┌──────────────────┐   ┌──────────────────────────┐
│ including:       │◄──│ Voivodeship      │◄─►│ The Voivodeship Crisis   │
│ Police, State    │   │ CMC              │   │ Management Team          │
│ Fire Service     │   └──────────────────┘   └──────────────────────────┘
└──────────────────┘

┌────────────────┐
│ Voivodeship    │
│ (regional)     │
└────────────────┘
```

```
┌──────────────────┐   ┌──────────────────┐   ┌──────────────────────────┐
│ Integrated       │◄──│  The Staroste    │──►│ Experts, other services  │
│ poviat services, │   │                  │   │                          │
│ inspectors and   │   └──────────────────┘   └──────────────────────────┘
│ guards,          │   ┌──────────────────┐   ┌──────────────────────────┐
│ including:       │◄──│ Poviat           │◄─►│ The Poviat Crisis        │
│ Police, State    │   │ CMC              │   │ Management Team          │
│ Fire Service     │   └──────────────────┘   └──────────────────────────┘
└──────────────────┘

┌────────────────┐
│ Poviat         │
│ (sub-regions)  │
└────────────────┘
```

```
┌──────────────────────────────────────────────────────────────┐
│ The voit (administrative officer of the commune), mayor        │
│ president of the city                                          │
└──────────────────────────────────────────────────────────────┘

┌──────────────┐   ┌──────────────────────┐   ┌──────────────────┐
│ Gmina        │◄─►│ The Gmina Crisis     │◄─►│ Experts, other   │
│ CMC          │   │ Management Team      │   │ services         │
└──────────────┘   └──────────────────────┘   └──────────────────┘

┌────────────────┐
│ Gmina          │
│ (lowest level) │
└────────────────┘
```

Figure 7. Structure of Poland's Crisis Management System (based on The Act on Crisis Management of 26 April 2017)

The Government Centre for Security ('RCB' in Polish) is the top level of planning in Poland, established at the national level. The RCB provides the service for the Council of Ministers, The Prime Minister and the Government Crisis Management Team. Ministers and regional authorities then implement the internal security measures set up their own Crisis Management Centres (CMC).

The obligation to initiate crisis management procedures is born by the authority that first receives the information that a crisis/threat has, or will, occur. This information should be immediately shared with the higher level authorities.

Exercise 5

Think about your country.
1. How is its crisis management system structured?
2. Draw a diagram of the system.
3. Discuss the differences.
4. Based on a SWOT analysis, determine the Strengths, Weaknesses, Opportunities for and Threats to the CMS in your country.

2.3. Response in crisis management

Fortunately, crisis situations can be recovered from, giving affected communities the opportunity to prepare for the possibility of further incidents. The best preparation is training and practical exercises.

The competence of the authorities and emergency services is very important in crisis management. The knowledge, experience and level of training of the decision-makers are also important. Training of crisis management participants should include the decision-making process, knowledge of legal provisions and the use of available tools and technical solutions. Another important part of preparedness is creating new trainers; teaching how to train others to handle crisis situations.

Training should not gloss over or avoid the mistakes and shortcomings of crisis management bodies, nor should it be perceived simply as a 'show' without clear goals, skipping over the realities and experiences of crisis situations. Instead, CM training should be designed to ensure that participants are fully prepared to make difficult decisions in stressful, complex situations. Apart from the primary goal of instilling individual and organisational competences, CM training should also enable the validation of existing procedures and action plans in crisis situations. In crisis management training, the following types of participants are distinguished:
1. Executives of government and self-government;
2. Managers and staff of administrative units, including shops and businesses assigned roles in crisis situations;

3. Employees of academic crisis management bodies.

The people and experts who actually arrange for and run training sessions are usually the same people responsible for crisis management at a given level (national, regional, community, etc). They are usually heads of their level of administration (managers, executives, etc), and it is part of their job to arrange for appropriate assistance and resources to assist the decision-makers in a crisis situation.

Training should be planned on the basis of an analysis of needs. This analysis should include: possible threats; associated risks; the characteristics and circumstances of the entity for which the analysis is being made; the executives' knowledge and available resources, and any identified deficiencies in the entity's crisis management plans. A good training plan should be based on a well-formed analysis of these needs, and notification of the training should clearly state the subject of the training, the date of its conduct, the persons/teams required to participate in the training, and the trainers who will be conducting it.

Along with regular training sessions, another highly effective form of preparation for all crisis management entities are field exercises. 'Real-world' exercises allow for comprehensive acquisition and maintenance of required levels of knowledge and skills by the staff of public authorities, institutions and aid organisations assigned roles in crisis response situations. Exercises create the conditions necessary to properly familiarise participants with possible crisis situations, the different variations of their roles in those situations and how to select the most appropriate response to each situation.

Exercises should be conducted periodically at all levels of crisis management and include all involved management bodies (decision-making, consultative, administrative, etc).

Exercises should be used to close out preparatory cycles, meaning that they should be run after the necessary training sessions have been conducted, so that they can also be used to check the effectiveness of the training. In this way, the exercises can be used to check the actual preparedness of CM participants for implementation of their tasks in a crisis.

Exercises should not be designed to be unnecessarily complicated. If participants spend most of their time trying to understand what's going on around them, they will not be concentrating on their objectives. As such, some elements of a real-world exercise should be invisible to those being tested. The principles of well-planned and executed field exercises include the following:

– The principle of **realism** – creating conditions as close to how they would really be as possible;

– The principle of **continuity** – ensuring the appropriateness of the objectives during the exercise;

– The principle of **confidentiality** – as far as possible, the content of the exercise must remain unknown to the participants, so as to properly emulate the unpredictability of a real situation;

– The principle of **safety** – despite the nature of a real crisis situation, exercises should not actually endanger the health and safety of the participants and property involved.

In the organisation and conduct of field exercises, a number of different people are involved:

– Exercise leader/commander;
– Exercise team/staff and managers;
– Back-up/support team;
– Observers/'referees' to guard against cheating or short-cuts;
– Security/assistants;
– Actors and other 'inside' personnel (playing victims etc.).

The first step in creating any good, effective CM training sessions and field exercises is to set out the concept. This should consist of:

1. Legal basis.
2. General description of the exercise:
   - Subject/theme;
   - Type of training/exercise: staff training/seminars; command and staff exercises; desktop training/exercise; live exercise; simulations, demonstrations;
   - A list of the objectives for the training/exercise.
3. A detailed breakdown of the objectives:
   - For the exercise/training leader (a single, broadly-defined objective);
   - For the training staff.
4. Stages, place and time of the exercise/training.
5. Scenario of the exercise/training.
6. Assets and resources to be used in the exercise/training.
7. Final provisions.

A basic exercise scenario should be:

– Realistic (based on events that have recently occurred and could happen again);
– Flexible;
– Simple;
– Designed to not create alarm or panic in the local communit.

After acceptance of the concept, the exercise leader should ask his team to prepare a more detailed document – a plan of the actual exercise on the day. This should contain:

1. Legal basis.
2. General characteristics of the exercise.
3. Detailed objectives of the exercise.
4. Entities involved and their cooperation with each other.
5. Stages, place and time of the exercise.
6. The assets and resources needed for the exercise.

7. Script (breakdown of the scenario, detailing actions and dialogue of actors etc.).
8. Participants' objectives.
9. Uniforms and equipment needed.
10. Safety conditions during the exercise.
11. Logistics of exercise first-aid and security resources.
12. Organisation of communications.

Exercise 6

Answer the following question: Do we really need exercises?

Exercise 7

Based on the preceding information, create an exercise concept. Use the following points as a guide:
Step 1 – What is the reason for this exercise?
Step 2 – What is the aim of the exercise?
Step 3 – Decide the participants' objectives.
Step 4 – Prepare the scenario.
Step 5 – Prepare some questions to tease out the objectives.
Step 6 – Driver inputs.

References

The Act on Crisis Management of 26 April 2017.

Banulska A., Sobór E., Iwańska M., *E-learning w zarządzaniu kryzysowym – platforma risko.e-ucz*, [in:] *Zarządzanie kryzysowe. Wybrane wyniki badań naukowych i prac rozwojowych*, Wyd. CNBOP-PIB, Józefów 2015.

Dillon B., *Emergency Planning Officer's Handbook*, Oxford Univ. Press, Oxford 2009.

Kaczmarek T.T., *Ryzyko i zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Difin 2005.

Kaczmarczyk B., Socha R., Szwajca A., *Zarzadzanie kryzysowe w systemie bezpieczeństwa publicznego*, Szkoła AspirantówPSP, Kraków 2014.

Perry R.W., *Disaster Exercise Outcomes for Professional Emergency Personel and Citizen Volunteers*, "Journal of Contingencies and Crisis Management", Vol. 12, No. 2, June 2012.

Procedure for Compiling a Fragmentary Report (an integral part of the spreadsheet) to the Report on Threats to the National Security, Government Centre for Security, Warsaw 2010.

Risk Management, Disaster Management and prevention against natural hazards in mountainous and forest region, 5D102 RIMADIMA an INTERREG III B CADSES NP project part financed by the European Union, Katowice 2008.

Rysz S.J., *Zarządzanie kryzysowe zintegrowane*, Difin, Warszawa 2016.

Skomra W., *Zarządzanie kryzysowe. Praktyczny przewodnik*, Presscom Sp. z o.o., Wrocław 2016.

Wolanin J., *Zarys teorii bezpieczeństwa obywateli. Ochrona ludności na czas pokoju*, War-
     szawa 2005.
Zarządzanie ryzykiem. Zasady i wytyczne, Polska Norma (PN-ISO 31000:2012), PKN,
     Warszawa 2012.
Zdrodowski B. (ed.), *Teoria zarzadzania kryzysowego*, Wyd. WSPol, Szczytno 2014.
Żmigrosdzki M., Zmigrodzki R., Żebrowki A., Michalczuk-Wlizło, *Zarządzanie kryzyso-
     we w państwie*, Warszawa 2012.