Dorota Leduchowska

Maciej Pyznar
Government Centre for Security, Warsaw, Poland

Critical infrastructure in Polish national risk assessment

Keywords

National Risk Assessment, Critical Infrastructure Protection, risk identification, risk analysis, risk evaluation

Abstract

Polish National Risk Assessment is produced every two years to identify, analyse and evaluate all risks which can cause a significant harm to the national security. Identified risks include natural disasters, major accidents and civil hazards as well as terrorism and other malicious attacks. Critical infrastructure might be destroyed or damaged as a result of events caused by the forces of nature or human action. Simultaneously, destruction or damage to the critical infrastructure might cause a serious threat to the state and the life of its citizens.

1. Critical Infrastructure

According to the Act of 26 April 2007, [1], on Crisis Management, critical infrastructure – is understood as - systems and mutually bound functional objects, including constructions, facilities, installations and services of key importance to the security of the state and its citizens, as well as serving to ensure efficient functioning of public administration bodies, institutions and enterprises. There are 11 critical infrastructures identified in the Act, [1]:
energy, fuel and energy resources supply systems,

- communication systems,
- tele-information network systems,
- financial systems,
- food supply systems,
- water supply systems,
- health protection systems,
- transportation systems,
- rescue systems,
- systems ensuring the continuity of public administration activities,
- systems for production, storage and use of chemical and radioactive substances, including pipelines for hazardous substance.

Critical infrastructure plays a crucial role in supplying key services to the society. Any disruption to each of the above mentioned supplied services might have a negative impact on the economic condition of the state as well as on its security.

Therefore, there is a legal obligation to protect critical infrastructure systems and risk assessment is an essential part of this process. According to the National Critical Protection Programme – "Risk assessment is performed with the use of the scenario-based method comprising the following steps, [3]:

- identification of threats and definition of scenarios,
- determination of a given scenario's probability,
- determination of the vulnerability of the CI and the protection measures,
- determination of the consequences of a given scenario,
- assessment of the risk of the CI damage in a given scenario.

All entities, both public and private, involved in CI protection are obliged to conduct risk assessment.
Moreover, risk assessment related to Critical Infrastructure is incorporated into the National Risk Assessment process.

2. National Risk Assessment

The first National Risk Assessment was conducted in 2011. As a result, a classified document called the Report on Threats to National Security was adopted by the Councils of Ministers. The legal basis for development of the Report are Act of 26 April 2007 on Crisis Management and Regulation of the Council of Ministers of 30 April 2010 concerning the Report on Threats to National Security. According to the

above mentioned legal acts, the Report consists of the following elements:

- Identification of significant threats (and their risk map);
- Definition of the strategic objectives;
- Capabilities and resources necessary to achieve the strategic objectives;
- List of projects (in hierarchical order) necessary to achieve the strategic objectives;
- Programs aimed at the improvement of the CI's safety and security;
- Priorities in responding to specific threats.

Each ministry, central agency and regional authority is legally obliged to monitor, analyse and foresee threats in the area of their responsibility. Therefore, preparation of the Report engages all government actors at both national and regional levels. It requires looking at threats and analysing them from different perspectives. Moreover, it provides an opportunity to compare risk perception at different levels as well as to develop a shared vision of major risks.

Government Centre for Security (GCS) is designed for the coordination of the national risk assessment process. It collects fragmentary reports prepared by ministries, heads of central offices and regional authorities. On the basis of these elements, it prepares a draft-Report on Threats to National Security. This document goes to the ministries, the heads of central offices and the regional authorities for approval. Once corrections and amendments are made, a draft-Report and a draft-proposal of respective regulations are transmitted to the Council of Ministers. The Report is approved by the Council by a regulation.

2.2. Risk identification

All governmental authorities prepare fragmentary reports. During this phase the widest possible spectrum of experts should be involved. This is when public sector should work together with private partners (especially critical infrastructure providers), academia and NGOs.

While producing fragmentary reports, the first step is to identify possible threats in the area of responsibility.

The Regulation specifies that the following kinds of threats should be taken into consideration:

- having a major influence on the functioning and possibilities of the development of the nation, in particular the threats of primary importance to international position as well as to national economy and defense potentials;
- whose effects can:
    - harm national security, its constitutional order, and in particular its sovereignty, independence and inviolability of its territory,
    - threaten a considerable number of people's lives, health, property or environment on a sizeable territory
    - impact on, in addition to Poland, other nations, as well harm the territory of Poland or its citizens although they might occur in another country,
- occurring in areas of tension, conflict and international crisis and impacting on the security of the nation's commitments towards signed contracts and international treaties;
- terrorist threats which can lead to a national crisis situation.

As Critical Infrastructure has a vital role in the functioning of the state and the lives of its citizens, destruction of Critical Infrastructure can be associated with all of the above mentioned types if threats.

2.3. Risk analysis

The Report is prepared in accordance with a methodology developed by the GCS [4]. Based on this methodology, for each identified threat public administration entity should indicate 2 – 3 scenarios together with the detailed description thereof. The description must include the potential location and possible causes (e.g. intentional or unintentional). Then, for each scenario, possible impacts on: population, economy, property, infrastructure and the environment are examined. For each of these categories both direct and indirect effects should be indicated. When analysing human impacts of a scenario the following categories are taken into account:

- potential number of fatalities;
- potential number of hospitalized (severely injured or ill);
- potential number of evacuated.

Secondly, potential impact on everyday life should be assessed. Besides, indirect social effects (unemployment, partial or permanent incapacity for work) as well as negative psychological effects should be considered.

Regarding potential damage to property and infrastructure possible potential cost should be assessed. Both direct and indirect costs need be taken into account (e.g. direct costs of restoration of a damaged building; indirect costs of business interruption resulting from damaged premises).

Moreover, potential harm to environment especially fauna and flora as well as to air, soil and water should be evaluated. It should be indicated whether

the adverse impact of a scenario is reversible or irreversible (causes permanent or long - term degradation of the environment) [9].
Ministries, heads of central offices and regional authorities should also analyse possible negative impacts on Critical Infrastructures, *Table 1*.
–In case of a damaged Critical Infrastructure a detailed description should be given, to what extent the Critical Infrastructure systems might be destroyed, damaged or its functioning may be disrupted. This is typically the failure modes, mechanisms and criticality analysis of systems.

Table 1. Ministers and heads of central offices responsible for each CI systems [2]

Critical infrastructure systems	Minister in charge of the critical infrastructure system
Energy, fuel and energy resources supply system	Minister of Economy Minister of State Treasury
Communication system	Minister of Administration and Digitization
Tele-information network system	Minister of Administration and Digitization
Financial system	Minister of Finance
Food supply system	Minister of Agriculture and Rural Development
Water supply system	Minister of Environment Minister of Administration and Digitization
Transportation system	Minister of Infrastructure and Development
Rescue system	Minister of Interior
System ensuring the continuity of public administration activities	Minister of Administration and Digitization
System for production, storage and use of chemical and radioactive substances, including pipelines for hazardous substances	Minister of Environment

According to the Programme they are responsible for "assessing the risk of malfunctions of CI systems caused by destruction or improper operation". Ministries should also analyse potential harm to CI systems under their responsibility and investigate the potential impact it might have on national security. This should be included in their respective contributions to the Report on Threats to National Security.
The next step in the preparation of the respective reports is to perform a global national risk analysis. For the purpose of the Report on Threats to National Security – risk assessment is understood as a combination of consequences of hazards (threats) and the associated likelihood of its occurrence [10].
The following qualitative description of the likelihood is used in *Table 2*.

Table 2. Qualitative description of the likelihood, [5]

Scale	**Likelihood**	**Description**
1	very rare	May occur only in exceptional circumstances. (once in five hundred years or even more rarely).
2	rare	It is not expected to happen. It is not documented at all. It does not exist in human communications. The events have not occurred in similar organizations, facilities, communities. There is a minimal chance, reason, or other circumstances that the events could occur. They may happen once every hundred years.
3	possible	It may happen within a certain time. Rarely random events that are documented or transmitted orally. Very few events. There is a chance, the reason, or the facilities causing the event to occur. It may happen once in twenty years.
4	likely	It is likely that it will occur in most circumstances. The events are systematically recorded and communicated in the oral form. There is a considerable chance, reason, or a facility allowing it to occur. It may happen once every five years.
5	very likely	It is expected to happen in most circumstances and/ or events are very well documented and/ or they operate among the population and are transmitted orally. May occur once a year or more often.

For assessing impacts the following qualitative (descriptive) scale is used in *Table 3*.

Table 3. Impact qualitative (descriptive) scale, [6] (Z - life and health, M - property, S - environment)

Scale	Impact	Cate-gory	Description
1	irrelevant 13.3%	Z	There are no fatalities or injured people. No one or a small number of people have been displaced for a short period of time (up to 2 hours). No one or a small number of people need help (no financial or material help).
		M	Virtually no damage. None or very little impact on the local community. Little or no financial loss.
		S	Imperceptible effect on the natural environment.
2	small	Z	A small number of injured people but no fatalities. First aid required. Necessary displacement of people (less than 24 hours). Some people need help.
		M	There is some damage. There are some obstacles (no longer than 24 hours). Slight financial loss. No additional funds required.
		S	Little impact on the natural environment for short-term effect.
3	medium	Z	Medical help needed but no fatalities. Some people require hospitalization. The extra space in hospitals and additional medical personnel needed. Evacuated people staying in the designated areas with the possibility of a return within 24 hours.
		M	Determination of the damage sites, which require routine repair. Normal functioning of the community with minor inconveniences. Considerable financial losses.
		S	Some effects on the natural environment but short-term or small effects with long lasting effect.
4	large	Z	Badly injured , a lot of people hospitalized, a large number of people displaced (for more than 24 hours). Fatalities. The need for specific resources to help people and to remove the damage.
		M	Community partially functioning, some services are unavailable. Large financial losses. Help from the outside needed.
		S	Long-term effects on the environment.
5	disastrous	Z	A large number of seriously injured. A large number of hospitalized. General and long-term displacement of populations. A large number of fatalities. Enormous help to a considerable number of people required.
		M	Extensive damage. The community's inability to function without significant external assistance.
		S	Large impact on the environment and / or permanent damage.

Each entity responsible for a specific report has to indicate possible likelihood and impact of damages and to score them from 1 to 5. When the likelihood and the impact are determined it is possible to assess the risk. It is indicated on the risk matrix. The risk level is determined by the colour:

- minimum (blue),
- low (green),
- medium (yellow),
- large (red),
- extreme (brown) [7].

2.4. Risk evaluation

The last step in preparing the respective ministerial reports is to determine the level of risk acceptance for each identified scenario. There are four categories of risk acceptance:

- acceptable - no additional measures are required. Current solutions and assigned capabilities and resources are sufficient. No additional monitoring activities are required;
- tolerable – the alternatives must be assessed as to whether the introduction of small organizational changes, either legal or functional, would contribute to the improvement of the safety or its public perception;
- conditionally tolerable risk - additional security measures should be introduced within six months, and the solutions used should be improved and approved;
- unacceptable risk - an immediate action to enhance security level ought to be taken, additional/new solutions should be introduced/provided and approved, [8].

At the end, for each scenario, the level of risk acceptance must be justified.

2.5. Strategic objectives

Identification of national security risks is an important strategic target. But equally important are the actions designed for risk reduction. Accordingly, both risk identification and corresponding actions are covered in the national security risk assessment report. In each individual ministerial report, the heads of central offices and the regional authorities are obligated to determinate what so-called the strategic objectives . For each identified risk, actions intended to either minimize the likelihood of a potential threat or mitigate its negative consequences needs to be outlined. Among the strategic objectives (targets), those classified at higher priorities should be clearly indicated. For all strategic objectives it is required to indicate both resources and capabilities necessary for their fulfilment.

The next step is to outline lists of necessary actions for achieving all strategic objectives (targets).
Ministries and heads of central offices responsible for Critical Infrastructure systems should incorporate in their respective reports the strategic objectives (targets) for ensuring the continuity of the services supply by the Critical Infrastructures.
Strategic objectives (targets) do mostly require long-term continuous policy actions. Actions necessary to achieve strategic objectives (targets) are more detailed and might be both structural (e.g.infrastructure updating/renewal investments) and non-structural (introducing new laws/regulations or improving early warning systems/surveillance procedures). They differ from emergency response procedures which are included in crisis management plans.

3. Emergency planning

The outcomes of the national risk assessment serve as a basis for civil emergency planning. According to the Act on Crisis Management, the conclusions of the report on the Threats to National Security are part of the National Crisis Management Plan (NCMP). They should be also included in the crisis management plans prepared by the individual ministries, heads of central offices and regional authorities.
The National Crisis Management Plan is designed for events where central government response is required (there is a lack of capabilities or resources at the regional level or there is a need for higher level of coordination of actions). The NCMP as well as the crisis management plans at regional and local levels contain inter alia of the following elements:
the characteristic of threats including those related to Critical Infrastructure, risk assessment of their occurrence, risk maps and corresponding hazard maps,

- the roles and responsibilities of different authorities (a security matrix),
- the capabilities and the resources which can be used to deal with emergencies,
- the threats monitoring process,
- the emergency response procedures, including those relating to the protection of the Critical Infrastructures,
- the organization of monitoring, warning and alarming systems,
- the crisis communications rules,
- the priorities in protection and restoration of the Critical Infrastructures.

Therefore, Critical Infrastructures protection plays a key role not only in the risk assessment process but also is an important part of the crisis management planning at all levels.

4. Conclusion

The report on Threats to National Security identifies the potential risks that may harm the Critical Infrastructures as well as outlines how destruction or damage of the Critical Infrastructures might cause a serious threat to the state national security and to the life of its citizens. The document should also give an insight into the inter-dependencies between the critical infrastructures.
Moreover, the Report provides a list of strategic actions aimed at reducing the risks. Some of those strategic actions are related to the Critical Infrastructure.
Additionally, Critical Infrastructures Protection (CIP) is integrated into emergency planning process at all levels.

References

[1] Act of 26 April 2007: http://rcb.gov.pl/eng/wp-content/uploads/2011/03/ACT-on-Crisis-Management-final-version-31-12-2010.pdf
[2] National Critical Infrastructure Protection Program, p. 28.
[3] Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego, Warszawa 2010: http://rcb.gov.pl/wp-content/uploads/procedura.pdf
[4] Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego, Warszawa 2010: http://rcb.gov.pl /wp-content/uploads/procedura.pdf, p.27 .
[5] National Critical Infrastructure Protection Program, p.18 .
[6] Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego, Warszawa 2010: http://rcb.gov.pl /wp-content/uploads/procedura.pdf, p. 32.
[7] Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego, Warszawa 2010: http://rcb.gov.pl/wp-content/uploads/procedura.pdf, p. 14.
[8] Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego, Warszawa 2010: http://rcb.gov.pl/wp-content/uploads/procedura.pdf, p. 15.
[9] Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego, Warszawa 2010: http://rcb.gov.pl /wp-content/uploads/procedura.pdf, p. 17.
[10] Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego, Warszawa 2010: http://rcb.gov.pl/wp-content/uploads/procedura.pdf, p. 18.