NATIONAL VOLUNTARY REVIEW OF
THE REPUBLIC OF POLAND
PRODUCED AS PART OF
THE MIDTERM REVIEW OF
THE SENDAI FRAMEWORK
2022
Publisher
The Government Centre for Security
Al. Ujazdowskie 5
00-583 Warsaw, Poland
e-mail: poczta@rcb.gov.pl
www.gov.pl/rcb

Authors
Beata Janowczyk
National Sendai Focal Point for Disaster Risk Reduction
& Head of Risk Assessment and Emergency Planning Unit
Government Centre for Security

Wiktoria Królikowska
Agnieszka Szajnert
Risk Assessment and Emergency Planning Unit
Government Centre for Security

Warsaw, 2022
The following report constitutes the contribution of the Republic of Poland to the Midterm Review of the Sendai Framework. The Government Centre for Security (GCS) as National Sendai Focal Point for Disaster Risk Reduction was responsible for the analysis and drafting of the report, building from the results of extensive consultation processes at the national and sub-national level. The GCS is responsible for supporting the Council of Ministers in crisis and risk management on the national level, and is the coordinating body for both the Report on Threats to National Security (RTNS) and the National Crisis Management Plan (NCMP). These documents set the agenda for risk reduction in Poland, and the NCMP functions as a crucial guiding document on risk planning and strategy.

Poland faces a range of disaster risks, from both natural and anthropogenic hazards. The most serious risk of disaster from natural hazards arises from flooding, heavy frost and snowfall, and drought. Wildfires also pose a risk in Poland, with a large number of fires clustered into a small area. Chemical contamination, radioactive contamination and disruption to gas systems are important anthropogenic and natech hazards. Geopolitical considerations also factor into Poland’s risk profile.

Poland has made strong progress in disaster risk management during the period of the Sendai Framework, but significant opportunities for improvement remain. Both risk understanding and risk governance are areas of strength in Poland, with risk assessments conducted systematically at the national and sub-national level. There is also a strong legislative and governance base of climate risk governance in Poland, supporting the coherent achievement of disaster risk reduction. Partnerships between sectors and levels of governance for integrated risk management is also an area of growing activity in the country.

Sufficient financing has been a key obstacle in the period from 2015 - 2022. At both the national and sub-national level, there have been consistent resource and capacity constraints in the implementation of disaster risk reduction activities. Further, there is a lack of a dedicated national strategy for risk management, which can hinder both the mobilisation of resources for and the coherent implementation of risk reduction activities in Poland. Further, reorganisation of governance bodies responsible for risk reduction presents an obstacle to informed and systematic risk reduction.

Looking forward to 2030, there is a need to build the awareness of multiple sectors of society to the language and practice of risk reduction. This includes expanding the institutional opportunities for government agencies and ministries to work with and learn from academic and non-governmental organisations. The creation of a unified legislative framework and the provision of increased financial resources have also been identified as important areas through which to accelerate and amplify the implementation of the Sendai Framework.

Finally, the Covid-19 pandemic was noted as a challenge during consultations and in open answers to the MTR survey by all entities that contributed to this report. Specific challenges created by the pandemic in the period from March 2020 included:

- The creation of additional workloads for government ministries
- The creation of new financial costs associated with safety regulations, including procuring personal protective equipment and increased costs of essential products
- A lack of education and understanding on procedure during pandemics
- Development of business procedures for online working, particularly for insurers
INTRODUCTION

Risk Profile - Natural Hazards

Flooding

Heavy Frost and Snowfall

Wildfire

Forest fires are currently one of the main causes of environmental damage in Poland. Compared to other European countries, Poland has a medium fire risk, but it is characterised by a large number of forest fires in a relatively small area.

Drought

Periodic occurrence of atmospheric droughts and the resulting soil droughts is a natural feature of the climate in Poland. Statistically, such a situation in Poland occurs once every 2-3 years. Atmospheric and soil droughts disappear relatively quickly, whereas hydrological drought generally lasts long, even several seasons, as rebuilding water resources requires abundant and long-lasting rain and snowfall.
Risk Profile - Natech and Anthropogenic Hazards

Chemical Contamination

Disruption of IT Networks

Radioactive Contamination

Disruptions in the Gas System

In the context of current and future disruptions to gas supplies due to geopolitical events, intense efforts are currently underway to diversify the sources of natural gas supplies to Poland. This could include the expansion of the LNG terminal in Świnoujście or construction of interconnections with the neighbouring countries.
OVERVIEW OF EXISTING RISK GOVERNANCE STRUCTURES

The Act on Crisis Management

Poland’s main law on risk assessment is the Act on Crisis Management (26 April 2007). Polish legislation defines ‘crisis management’ as a comprehensive process incorporating risk prevention, preparedness, response, and recovery. The risk assessment process is considered inter alia as part of the prevention phase, informing the other phases along the way. The Act describes the planning cycle for crisis management as ‘periodic implementation of the phases of analysis, programming, the development of the plan or programme; its implementation, testing and initiation’. However, the definitions in the Act should be aligned with those used in the EU Civil Protection Mechanism guidelines.

The Act on Crisis Management sets out the responsibilities on all four government levels (local: municipalities and counties, regional and central); the general principles for crisis management, and the rules on financing crisis management tasks. At the highest level, the Council of Ministers is responsible for crisis management. In the event of a crisis, a Government Crisis Management Team is set up under the Council of Ministers, with the Prime Minister acting as chairman. This Team is supported by the GCS which is established in the form of a state budget unit under the Prime Minister and also serves as a national centre for crisis management. Its Director is appointed by the Prime Minister and acts as secretary of the Team.

The Report on Threats to National Security

The Act also governs the assessment of threats and risks. For the purposes of the National Crisis Management Plan (NCMP), ministers in charge of the government branches, the heads of central offices and the voivodes (regional level) have a legal obligation to contribute to a Report on Threats to National Security (RTNS), by means of fragmentary reports. The Director of the GCS has to ensure the overall coordination of the preparation of the Report, while the Head of the Internal Security Agency is responsible for the coordination and preparation of the part relating to terrorist threats. In case of the cyberspace threat coordinating body is the Government Plenipotentiary for Cybersecurity.

This Report concerns the most significant threats, and has a major influence on national development. It is particularly influential in its assessment of primary security threats, their implications on Poland’s international position as well as its economic and defensive potential, and also their threat to a considerable number of people’s lives, health or environment. The aim of the Report is to assess, compare and select major risks to national security. As some information may be regarded as classified for security reasons, the RTNS is restricted (lowest level of classification). Based on the RTNS, the GCS adjusts the risk assessment at national level and gives conclusions at appropriate sub-national level. In the event of a discrepancy between central and provincial risk acceptance levels, a two-way phase level is adopted whereby a discussion is entered into and a compromise is reached.

Risk assessment also proceeds up through the government structure from the subnational level. First, risk assessments are shared from gminas (municipalities) and poviat (counties) to voivodeships (provinces, region), and second, from voivodeships to central government, with the GCS acting as the central coordinating agency. For the purposes of civil protection and security, the 16 voivodeships are responsible for policy in their geographical area. They are required to develop a fragmentary report for their area, on which the GCS provides feedback. These reports are eventually integrated into the RTNS. Lower level entities usually follow the GCS guidelines.

Voivodeships in turn take account of assessments at poviat and gmina level. Local stakeholders carry
out their own assessments, but risk assessment at local level has a weaker legal base. The Act is not explicit on assessment at local (powiat, gmina) levels. Local crisis management plans are subject to voivodeship supervision and evaluation. There is a general risk assessment recommendation for self-governing entities to address probability, effect, scale, and impact. In general, entities at the lower level of government assess a wider range of risk scenarios.

National Crisis Management Plan

The National Crisis Management Plan (NCMP) a planning document prepared by the GCS in cooperation with ministries, central offices, and voivodeships. It can be regarded as a crisis management manual for planning at the central level. As a planning document, NCMP serves the administration responsible for crisis management at the central level. The National Crisis Management Plan is created for all four crisis management phases. The conclusions of the RTNS are not only part of the NCMP, but are also included in all other crisis management plans at all levels of government. Each ministry and public agency referred to in the Act on Crisis Management has to develop its own sectoral crisis management plan taking account of the RTNS. To link central and local planning processes, the crisis management plans (and the risk assessments on which they are based) have to be approved at higher government level (in the case of municipalities/poviatas, by the voivodeship; in the case of voivodeships, by central government).

For each of the national threats, lead and support responsibilities for the four phases are clearly defined in a security matrix as part of the NCMP. The division of responsibilities for each risk is available at national and regional/local levels. This is based on an analysis of the RTNS, followed by legal acts or context analysis resulting in a proposal designating lead and support entities. However, the security matrix does not reflect co-owned and shared risks to be addressed in a multi-hazard ‘whole of government’ approach taking into account cascade effects and long term consequences. If an emerging risk is not ‘owned’ by a specific sector, the Government Crisis Management Team proposes to the Council of Ministers that it be assigned to a particular ‘owner’. The objective is to ensure that every risk is owned by a leading stakeholder; that stakeholder is identified as the owner and is made accountable for the risk.

The National Water Agency

The National Water Agency is responsible for supervising preparation and implementation of River Basin Management Plans, Flood Risk Management Plans, and the National Programme for Urban Wastewater treatment. It is also responsible for supervising water planning governance structures, including the National Board for Water Management in Warsaw, and Regional Water Management Boards. Regional Water Management Boards are responsible, inter alia, for:

- Identifying significant pressures and assessing their impact on the status of surface and groundwater in the region,
- Preparing flood studies in the region and developing draft plans for flood protection,
- Coordinating activities related to the protection against floods and drought
- Develop economic analysis of water use in the region

Risk Management Plans

Unfortunately, there is no existing obligation in the Polish law to prepare risk management plans and strategies for disaster risk reduction. However, the RTNS and the NCMP consist not only of risk assessment but also risk management and can be regarded as a National Risk Management Plan and a Strategy for Disaster Risk Reduction at the central level. In addition, the fragmentary reports for
RTNS prepared by the voivodes could be considered to function as Regional and Local Strategies for Disaster Risk Reduction.

**Critical Infrastructure**

One of the most important strategic documents in the area of increasing the resilience of critical infrastructure systems in Poland is the National Critical Infrastructure Protection Programme (NCIPP). The NCIPP defines the vision and the objectives behind critical infrastructure protection processes and covers all the phases of the risk management cycle: it aims not only to ensure critical infrastructure’s protection against threats (prevention), but also to contribute to the reduction of the impact and length of the potential damages (preparedness and response). The NCIPP addresses the following infrastructure systems: energy, communication, ICTs, financial, food supply, water supply, health protection, transportation, rescue, public administration and the production, storage and use of chemical and radioactive substances. The NCIPP describes the cooperation to be set between individuals, and sets out roles and responsibilities for each stakeholder. The NCIPP pays particular attention to building partnerships between stakeholders. The document recognises that information and knowledge sharing between all levels of the administration as well as between the public and the private sector are key in protecting infrastructure systems. The NCIPP also identifies a number of good practices and recommendations to ensure the smooth functioning of critical infrastructure, in several areas such as technical protection, IT/OT protection, legal protection, business continuity/recovery plans.

As part of efforts aimed at enhancing the level of protection of critical infrastructure in Poland from unmanned systems (also known as drones), the ‘Security Standards for critical infrastructure operators in preventing, responding to and reducing the effects of threats posed by incidents involving unmanned systems’ has been developed. The material was created by the Inter-ministerial Unmanned Systems Security Standards Team, established at the GCS.

**METHODOLOGY**

The methodological approach for Poland’s Midterm Review proceeded in three stages:

1. Questionnaires with closed and opened questions were sent to Ministries, regional entities, critical infrastructure operators, scientific research institutes and universities, NGOs and public administration officials. 200 answers to questionnaires were analysed by the GCS.
2. A process of qualitative interviews was conducted with the entities that received the questionnaire, to allow the sharing of in-depth and expert viewpoints
3. Two consultation meetings were held, to exchange views and contribute to the analysis of the report. On the 5th of July, a meeting was held with public administration entities at central and regional level. On the 20th of July, a meeting was held dedicated to scientific research institutions, NGOs and insurers.

The MTR process in Poland also made use of the results of the United Nations Disaster Risk Reduction Capability Stress Test report from 2022, as well as analysis of statistical and historical data, and bilateral interviews with experts in risk management.
RETROSPECTIVE REVIEW

Understanding

Strengths
There are a variety of activities pursued across government institutions that support a better understanding of risk in Poland. These include trainings and conferences for risk management professionals, and competitions for children and adults centred around risks emerging from climate change.

94% of surveyed institutions note that they monitor disaster risk. This is achieved through a variety of techniques, dependent on an institution's mandate and expertise. These include dedicated monitoring and reporting systems for hazards and threats, monitoring of social media, technical simulation tests and specific risk analysis processes. 44% of surveyed institutions explicitly include climate change as a factor in their risk assessment, assessing potential impacts from hurricanes, drought and severe frost.

The Information Space Security Team at the GCS has developed a number of projects to prevent disinformation, ranging from work focusing on building an information society through education to projects concerned with social resilience. The team monitors traditional and social media for information about emerging risks, as the GCS prepares analysis and recommendations for actions that are communicated by key public institutions. The four main activities of the team are: recognition of alien actors in Polish-language information space; recognition and analysis of the methods used by such actors; monitoring of risks in the information space, including multi-domain and hybrid; and analysis and planning of actions to mitigate risks. The GCS Disinfo Radar and the GCS Academy Project support the education of broader society on risk and its mitigation. The Government of Poland is therefore active in promoting risk understanding by combating disinformation.

Obstacles
A key obstacle to appropriate management of risks in Poland is a continuing lack of knowledge and competence at multiple levels of government in controlling and enforcing risk reduction activities. Only 19% of surveyed government institutions make use of satellite imagery in assessing and managing risk. As a result, it was agreed by 100% of institutions and 100% of surveyed Voivodeships that there is a pressing need for a national level GIS to provide support in this area. The development of GIS National Security was undertaken in direct response to this need.

There is a systematic lack of reporting on data relevant to disaster risk in Poland: only 19% of relevant institutions noted that they keep databases with information pertaining to losses caused by disasters. At the Voivodeship level, the number increases to 55%.

There is also a lack of competence in risk management techniques in the general population. This is evidenced by difficulties in employing people with appropriate qualifications. 81% of institutional respondents identified improving education on disaster risk and resilience as a key priority in managing risk going forward.
Governance

Strengths

Sub-national risk governance

Sub-national governance in Poland is structured around the unit of the Voivodeship. In total, there are 16 Voivodeships in Poland, of which 9 responded systematically to the Midterm Review survey.

Risk Understanding:
- 100% of Voivodeships that responded to the survey report that key risks are monitored at the sub-national level
- 100% of Voivodeships that responded to the survey include threats to critical infrastructure in their risk assessment process, and 89% include cascade effects
- 75% of surveyed Voivodeships have cooperated with local governance structures to provide and support risk assessment services in the past three years
- 55% of surveyed Voivodeships maintain databases recording losses from disasters. 77% engage in some form of reporting of losses from disasters to the national level.
- The Provincial Crisis Management Team (WZZK), the GCS and the Institute of Meteorology and Water Management - National Research Institute (IMGW) are the key sources of information on hazards and other threats at the Voivodeship level

Risk Governance:
- Voivodeships employ an average of 15 employees in the area of crisis management
- 77% of surveyed Voivodeships have adopted a strategic plan to reduce risk in the period from 2015 - 2022, though the focus is often on climate change, mass migration and evolving threats to health rather than disaster risk reduction

Risk Financing:
- 100% of surveyed Voivodeships indicate that funding for risk reduction has increased by 1 - 25% in the period from 2015 - 2022
- 67% of surveyed Voivodeships have financed education and awareness raising campaigns, the adoption of new technologies by crisis management teams, and measures to ensure business continuity in times of crisis from their budgets from 2015 - 2022.
- The majority of financing for Voivodeship-level risk reduction comes from the state budget, with the European Union a secondary contributor

Indicative activities of Voivodeships from 2015 - 2022:
- Development of a new Voivodeship Crisis Management Plan
- Provision of guidelines to local government units in the field of crisis management

The key challenge for risk governance at the sub-national level from 2015 - 2022, noted frequently by Voivodeships, has been a lack of sufficient financial and human resources to effectively implement risk reduction activities. Further, only 22% of surveyed Voivodeships finance activities that also address climate change risk from their existing budget. In the period to 2030, 100% of surveyed Voivodeships believe that the priority area for risk reduction is a more thorough education of society on topics of risk management, supported by cooperation with NGOs and scientific institutions, and the adoption of new technologies.
Climate Risk Governance

It should be noted that Poland has been taking action for many years to adapt to climate change and counteract the adverse effects of this phenomenon. The Republic of Poland participates, among other things, in the implementation of the projects referred to in the following:

- The Sendai Framework for Disaster Risk Reduction 2015-2030 adopted at the Third UN World Conference held in Sendai, Japan, in 2015;

The Government of the Republic of Poland and Polish public administration bodies initiate and support the introduction and implementation of various projects in this area. Examples of this type of action may include:

- The programme Adapting to climate change and reducing the effects of environmental threats, implemented between 2015 and 2025;
- Stop Drought! project - Plans to counteract the effects of drought, implemented in 2016 – 2020;
- The Clean Air programme for 2018 – 2029;
- Alert RCB, a system of SMS notification of threats to the public, used only in emergencies where there is a high probability of an immediate threat to life or health in a significant area. The project’s implementation started in 2018 and is ongoing;
- My Electricity Programme – initiative launched in 2019;
- Programme for Counteracting Water Scarcity for 2021-2027 with a 2030 perspective.

Further, there are long-term strategic documents that deal with the realisation and management of climate risk:

- Strategic Adaptation Plan for climate-sensitive sectors and areas by 2020 with a 2030 perspective
- The 2030 Polish National Environmental Policy - a development strategy for the environment and water management, containing climate scenarios in line with the forecasts of the Fourth and Fifth Report of the Intergovernmental Panel on Climate Change (IPCC) 8.

Looking forward, 50% of surveyed institutions identified adaptation to climate change as a key priority for resilience in Poland.
Obstacles

- Lack of unification in the legal environment in terms of crisis management has been identified as an important obstacle to the implementation of the Sendai Framework in Poland. This lack of unification means that the issue is not fully regulated.
- At the level of sub-national governance structures there is insufficient financing for risk management, as well as a lack of engagement with non-governmental organisations and limited means for exchanging risk information.
- The new challenges like pandemic, cyberattacks, migration crisis that we have faced during the recent years have indicated that the vertically integrated approach in Critical Infrastructure is not advanced enough. It is therefore important to correctly identify, understand, analyse and draw conclusions from new challenges in order to implement practical measures to build resilient infrastructure. UNDRR’s stress-testing tool allowed Poland to identify sensitive areas and identify potential solutions for disaster prevention and resilience building, with a specific focus on Critical Infrastructure. It is improving cooperation between administration and critical infrastructure operators by creating an established process of sharing good practices and needs.

FINANCING

The financing of actions to manage natural disasters and catastrophes is a complex area. In accordance with the Act on Crisis Management, the state budget provides for the financing of crisis management tasks at national level, and part of the funds is at the disposal of the voivodes. Municipalities, poviats and voivodeship self-government administrations have to finance their tasks in the field of crisis management from their own budget, but they also can receive subsidies from the state budget including funds for the rebuilding of their infrastructure or direct help for the population. The state budget provides for an annual reserve for prevention and removing consequences of natural disasters. Local authorities have to satisfy certain criteria in order to receive funds. Plans have to be submitted determining the manner of returning to the original state and accounting for changes allowing for avoiding repeated damage caused by a threat of a similar scope.

Financing for risk reduction and resilience is distributed across different government agencies. 81% of surveyed institutions committed resources to improving education and awareness on risk from 2015 - 2022, whilst 75% invested in ensuring business continuity in the event of disaster. This is an area of increasing momentum: 69% of surveyed institutions called for increased attention to business continuity in moments of crisis as a key step in increasing resilience to disasters in the country. From a technological perspective, 56% invested in improving technology to prevent and address crises, and 94% invested in improving the resilience of their information technology systems. However, only 25% committed institutional resources to adapting to the effects of climate change.

Despite these provisions, agencies active in risk management have identified a limited budget as a key obstacle to the implementation of the framework from 2015 - 2022. Over one-third of surveyed ministries noted that the budget available for risk management was simply insufficient. The limitations in financing for entities responsible for risk management has led to high staff turnover and the reorganisation of the Risk Assessment and Emergency Planning Unit mobilisation. More broadly, the...
lack of a dedicated crisis management financing stream at national level creates a significant capacity constraint with regards to the implementation of the Sendai Framework. This capacity limitation is also experienced by other institutions across government: only 12.5% of surveyed institutions report forthcoming significant investments in improving infrastructure.

### Financing for risk reduction and resilience

<table>
<thead>
<tr>
<th>Risk Management Area</th>
<th>Investment Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adapting to the effects of climate change</td>
<td>25%</td>
</tr>
<tr>
<td>Improving the resilience of their information technology systems</td>
<td>94%</td>
</tr>
<tr>
<td>Improving technology</td>
<td>56%</td>
</tr>
<tr>
<td>Ensuring business continuity</td>
<td>75%</td>
</tr>
<tr>
<td>Improving education and awareness on risk</td>
<td>81%</td>
</tr>
</tbody>
</table>

*Figure 9: the percentage of surveyed government institutions that invest in different aspects of risk management*

### PREPARDNESS AND EARLY WARNING

A key success in this area is Alert RCB, Poland’s SMS-based early warning system. Alert RCB is an example of cooperation between decision makers and scientists, due to its joint development with research entities in the field of threats monitoring and citizens warning. The SMS system is used to warn citizens of dangerous events but also to increase public awareness of threats arising from climate change. In 2021, 507,749,369 messages were sent in Polish and 36,839,568 in English. An important supplementary tool that allows the sensitization of the population about local threats is the Regional Warning System. As part of this system, messages about potential threats created by voivodeship crisis management centres, appear on TV screens, on the website and in the mobile application. The early warning system in Poland is an example of a risk management technique that both responds to acute instances of disaster and works more generally to build a more resilient society. It also demonstrates the necessity of working closely with research entities for risk reduction, as it is the product of close collaboration between government and academic entities.

To supplement Alert RCB and the Regional Warning System, and to support communication in situations of disasters, the GCS also created the Crisis Communication Book. This compendium of experiences of crisis scenarios and media strategies includes a template press release and sample responses to challenging questions from journalists. Another example of educational materials related to crisis management is GET READY! Guide for Crisis and War, produced by the Academy for Security. Through these initiatives and other means, the Government of Poland works to educate and increase the preparedness of citizens in the context of major threats.
Regional collaboration is an area of strength in Poland. Initiatives such as the Lublin Triangle, V4 and the Network of Director General of the European Crisis Management Centre serve to support the identification, comprehension and analysis of risks and the development of coherent measures to build resilient infrastructures. The stress testing programme prepared by UNDRR-ROECA, which seeks to assess resilience capability taking into consideration key indicators from various sectors, is a further example of this emphasis on international partnership.

Science and Academia
An example of good practice in Poland from 2015 - 2022 concerns a more structured and institutionalized collaboration between science and public administration:

- The Government in cooperation with scientists implemented a data integration platform using Geographic Information Systems software (GIS National Security) for the crisis management system. The point of developing GIS National Security is to create a database of losses caused by disasters to fulfil implementation of the Sendai Framework but also to assess and manage risks locally.
- The Government worked on the prognostic models of coronavirus spread in Poland with the Mathematical and Computer Modelling Centre of the University of Warsaw. This tool allows government personnel to share data with research and development entities, and generate analyses, forecasts, scenarios modelled by use of AI. This data was shown in the GIS National Security system.
- The Government (including the GCS) cooperated with the Space Research Centre for Polish Academy of Sciences to build a platform integrating different services in one place – satellite imagery, data collected by drones and other maps tools - to improve our early warning system and to build situation awareness amongst decision makers.
- The Prime Minister’s Medical Council, established during the pandemic, is another venue for collaboration between public administrators and scientists. Scientists and policymakers speaking with one voice is a crucial way of fighting disinformation.

This qualitative emphasis is supported by the quantitative data. 56% of surveyed administrative institutions report connections with scientific and research institutions. These connections include experience sharing, joint research and training ventures, and work counteracting the effects of drought. Surveyed voivodeships reported progress in this area from 2015 - 2022, with multiple sub-national governmental units reporting collaboration with Polish universities and research institutions towards risk reduction, especially in the form of education and capacity building.

However, there is work to be done to improve the structure of this relationship. A lack of guidelines and programs that specify the conditions for cooperation with scientific and research organisations is a barrier to a fuller integration of these actors into risk governance in Poland. More generally, 56% of surveyed institutions identify an improved relationship with the world of science as a key priority for improved resilience in Poland. This is reflected in a survey conducted by the GCS, which underscored that there is extremely limited collaboration between the regional level and scientific research institutions.
Private Sector
44% of surveyed institutions report collaboration with the private sector in the area of risk management. These collaborations stretch across a broad range of areas, determined by the government institutions core mandate and competencies. They include partnerships to strengthen cybersecurity, to improve control of construction works, to provide support on business continuity and improvement of research methodologies. Critical infrastructure operators noted a closer cooperation with distributors, voivodeships, emergency services and the school system. This cooperation is supported by the annual National Forum for Critical Infrastructure Protection and National Forum for DRR. These platforms are strong examples of private-public partnership aimed at educating people at different levels, to inspire them and encourage them to create bottom-up initiatives to improve resilience.

A survey conducted by the GCS revealed a systematic lack of engagement with non-governmental institutions and volunteers on the local level. In total, over 30% of institutions surveyed for the MTR recognised improving collaboration with non-government organisations as a key priority in improving disaster resilience in the country. Analysis also revealed a need for building even better cooperation between entities on different levels that could solve the problem of partially limited coordination of information exchange. An important venue for this cooperation is the annual National Forum for Critical Infrastructure Protection and the National Forum for DRR, which work to realise the principle of private-public partnership in order to educate people at different levels, and to inspire them to develop bottom-up initiatives to improve resilience.

In their inputs to this Midterm Review, entities at the central and regional level, scientific researchers and critical infrastructure operators described new cooperation opportunities coming from the pandemic experience. More than half of respondents in each one of these categories noted a substantial increase in cooperation between their institution and other entities as a result of the pandemic. From a scientific perspective, it was a period of very intense research, with the possibility of sharing scientific findings with central, provincial and private sectors. Public administration organisations frequently shared information about their problems and turned to academic and research institutions for solutions, such as modelling of cascade effects. The connections that were created during the pandemic period have created a framework for further institutional collaboration.
The GCS in Poland, as National Sendai Focal Point for Disaster Risk Reduction, is constantly working on implementing new technologies in crisis management and disaster risk reduction, as well as cooperating with scientists in this area. Every disaster is an opportunity. COVID-19 was a chance to test systems that the GCS had already been developing, and to create new ones driven by lessons learned. COVID-19, both in its realisation and in the responses it catalysed, was the key context shift in the period 2015 - 2022.

The pandemic demonstrated clearly how important cross-sectoral cooperation is, and has also stressed how significant is the need to tighten the cooperation between CI operators and decision makers. At the beginning of the COVID-19 pandemic, GCS created a geo-information system for crisis management units involved in fighting against COVID-19. The purpose was to provide the necessary data, present the forecasts of the epidemic’s spread in Poland and offer the public access to an up-to-date map and information published on the governmental website. The system, managed by GCS, was the result of cooperation among many governmental entities, the private sector and the world of science. Another functionality of the system was an ‘availability of beds’ application, that delivered data to rescue services about vacant COVID-19 beds in hospitals, to enable the quick redirection of ambulances carrying COVID patients in need of intensive care.

The system, named GIS National Security, is an effective tool beyond the context of pandemics. It is useful for counteracting various hazards at all phases of the crisis management. The main goal is to build situational awareness by monitoring and analysing the most important threats to national security, including those related to the war in Ukraine. GCS has created a tool allowing us to share the data with research institutions, and provide analyses and scenarios modelling by artificial intelligence. Those products are shared with entities responsible for crisis management and civil protection, scientists, services and also decision makers. The system provides a means to integrate different services in one place – satellite imagery, data collected by drones and other maps tools. This improves Poland’s early warning system and builds threat awareness amongst decision makers. Satellite and drone images were used to monitor wildfires in Poland’s largest national park (Biebrza National Park) in 2020 and a heavy ice jam on Vistula river creating the risk of flooding areas near Włocławek Reservoir. The system is also a tool to collect the data on losses from disasters to report to Sendai Framework Monitor. See below for representative examples from the dashboard of GIS National Security.
Figure 10: Dashboard 1. Portal for citizens in GIS National Security – epidemiological situation.

Figure 11: Dashboard 2. Portal for citizens in GIS National Security - vaccination process.
Other Context Shifts
From 2015 - 2022 it has become clear that, in the modern world, we are less and less often faced with homogenous and isolated threats. Most often the threats occur in various combinations, with the emergence of one threat frequently initiating another one or more. Attempts to introduce (or stick to old) strict divisions are doomed to failure or, at best, to a situation in which the same threat can be classified in more than one category. The boundary between civilisation threats and those caused by intentional human activity is particularly blurred. In addition, the situation is complicated by the fact that many identical threats may have not homogenous sources of their origin even in the same territory/area. In order not to artificially separate the civilisation threats from those resulting from intentional human activity, the following risks should be understood as interlinked with each other and with natural hazards:

- Disruption in the fuel system (liquid fuel supplies);
- Disruption in the gas system (gas supplies);
- Disruption in the electricity system (electricity supply);
- Disruptions in telecommunication systems and services;
- Disruption in IT systems and services;
- Maritime disasters
- Chemical contamination on land;
- Chemical contamination at sea;
- Radioactive contamination;
- Collective disruption of public order;
- Mass migration;
- Hybrid activities.

In particular the growing threat of cyber attacks has been noted by colleagues throughout government as a point of increasing concern from 2015 - 2022. This has been mirrored by an increasingly developed use of cyber security techniques and other new technologies by government entities. As digital
technologies become more sophisticated and geopolitics more polarised, it is likely that this trend will continue in the years to 2030.

2022 - 2030
Institutional informants for this Midterm Review identified a range of processes which will shift the context for the implementation of the Sendai Framework and risk management more broadly in the years from 2022 - 2030. They are presented below, ranked from most to least widely noted:

- Hybrid threats that combine military and non-military means
- Disinformation
- War
- Increasing frequency of natural hazards such as flooding and droughts
- Migration crisis
- Epidemics
- Climate Change
- Threats to energy production
- Cyber security threats
Understanding

Looking forward, a very important issue is building a social consciousness of the nature of DRR. This matter was specifically underlined by scientific research and critical structure entities that provided inputs for this report. It is also a conclusion from an analysis of answers from the provincial level, as some of the institutional respondents did not completely understand a question about DRR and building resilience. Further, during the UNDRR-supported stress-testing process, some of the tasks were identified as unclear due to a lack of clarity over terminology and translation. It is therefore essential to educate society and create a universal comprehension of disaster risk reduction.

- Accelerate sensitisation and capacity building of key decision-makers to disaster threats, including processes which structure vulnerability to disaster
- Ensure periodic central training on for government employees on crisis management
- Implement a national risk assessment methodology and process as a starting point for developing and systematising risk management activities, with an obligation for entities to prepare risk management plans
- Foster broader availability of analytical tools in governance institutions to support understanding of disaster risk
- Create a statutory obligation for insurance companies and emergency services to support analysis through the provision of risk data
- Educate of all members of society about disaster threats

Governance

- Implement the obligation to draw up plans in legislation on risk management. The development of a coherent system of hard laws and regulations to support risk management authorities and practices is crucial to the creation of a sustainable culture of risk prevention and reduction. These plans should include an explicit commitment to the Sendai Framework
- Develop comprehensive regulations on crisis management and civil protection. These regulations should provide guidelines to create coherence and unity of decision-making bodies, with a single crisis management centre to coordinate between other bodies.
- Integrate risk governance planning with development planning, protection planning and business continuity planning
- Ensure consistency and collaboration between crisis management authorities and systems for security and defence
- Simplify and streamline the risk governance structure, including through a more efficient planning system
- Intensify efforts to construct a disaster-proof society, including through building codes and land use planning
Financing

- The key step to take is a broad and sustained increase in the amount of funding available for risk reduction activities, as part of an increased priority for risk governance activities.
- Increase investment in human and technical capacity for risk management at the national level
- Ensure that risk insurance assessments and disbursals are based on sound risk assessment methodologies
- Tax and welfare policy should ensure the burdens and allowances are dependent on financial means, strengthening resilience to disaster amongst the poorest in society
- Make government investments conditional on a project fulfilling preparedness and climate-risk reduction criteria

Partnerships

- Analyse the existing legislative framework to identify opportunities for central government cooperation with non-governmental organisations and research institutions
- Create new legal frameworks, platforms and institutions to facilitate the mainstreaming of non-state actors into the risk management process at the national level
- Involve scientists to support the implementation of European Civil Protection Mechanism through the development of a national risk assessment including threats analysis linked with climate change scenarios.
- Strengthen short-term cooperation with scientific and research institutions to plan for various forms of threats is a key priority, including through their inclusion in crisis management exercises
- Increase research funding and direct funding to non-governmental organisations to support work on disaster resilience
- Cooperate with a variety of governmental and non-governmental partners in the field of awareness raising for resilience