INSTYTUT POLITYKI ENERGETYCZNEJ IM. IGNACEGO ŁUKASIEWICZA

ANALYSIS NO. 5/2022

PROTECTION PLAN FOR ENERGY INFRASTRUCTURE IN TERMS OF MARINE WIND ENERGY DEVELOPMENT IN THE MARINE AREAS OF POLAND

Tomasz CHYŁA[1]

[1] Cmdr Lt. M.Sc. Tomasz CHYŁA, senior lecturer at the Department of Command and Maritime Operations at the Bohaterów Westerplatte Naval Academy in Gdynia, expert at the Ignacy Łukasiewicz Institute for Energy Policy in Rzeszów.

POSSIBLE THREATS TO MARINE WIND FARMS

Bearing in mind the events that took place in September this year in the Baltic Sea (in close proximity to the Polish Exclusive Economic Zone), i.e. the confirmed sabotage of the Nord Stream gas pipelines, as well as the latest Polish Wind Energy Association (PWEA) calculations included in the report "The Potential of Offshore Wind Energy in Poland", stating that by 2040, by using the total estimated potential of the Polish part of the Baltic Sea, offshore wind energy could meet up to 57% of the total demand for electricity in Poland, it can be successfully concluded that our country's energy security will be largely based on offshore renewable energy installations, which will be vulnerable to various threats and, as yet, almost entirely unprotected. In order to cope with the growing challenges and threats, in the marine domain (both the water column and its lower hemisphere), which is difficult to monitor and exercise effective protection in, it is necessary to be aware of the scale of possible threats and to prepare an appropriate response strategy. The lack of an official definition of "offshore wind" in Polish maritime areas is not a reason not to prepare a counter-response to the possible risks during the more than 30 years of exploitation (construction, operation and decommissioning phases). The protection of this infrastructure, in view of its strategic importance for the Polish energy sector and thus for the Polish economy and its competitiveness, should be considered through the prism of Polish legislation and the guidelines from the Government Security Centre.

CRISIS MANAGEMENT AND OFFSHORE WIND

In the Crisis Management Act of 26 April 2007 (CMA), critical infrastructure protection is defined as all activities aimed at ensuring the functionality, continuity of operations and integrity of critical infrastructure in order to prevent threats, risks or vulnerabilities and to reduce and neutralise their effects, as well as restoring such infrastructure rapidly in the event of failures, attacks and other events that disrupt its proper functioning.

Pursuant to the provisions of Art. 5. 1. of this Act, a National Crisis Management Plan and voivodeship, district and municipal crisis management plans, hereinafter referred to as 'crisis management plans', are established, which include, *inter alia*: functional annexes of the master plan defining the procedures for the execution of crisis management tasks, including those related to the protection of critical infrastructure.

In turn, Art. 5b. 1 indicates the adoption (by Resolution of the Council of Ministers), of a National Programme for the Protection of Critical Infrastructure, the aim of which is to create the conditions for improving the security of critical infrastructure, in particular with regard to:

1) preventing the disruption of critical infrastructure,
2) preparing for crisis situations that may adversely affect critical infrastructure,
3) respond to situations concerning the destruction or disruption of critical infrastructure,
4) restoration of critical infrastructure.

Art. 6. 1 specifies critical infrastructure protection tasks, which include:

1) collection and processing of information on critical infrastructure threats,

2) developing and implementing procedures in the event of critical infrastructure threats,
3) restoration of critical infrastructure,
4) cooperation between public administration and the owners and possessors, whether legal or natural persons, of critical infrastructure installations or equipment as regards their protection.

In addition, owners and possessors of critical infrastructure facilities, installations or equipment have an obligation to protect them, in particular by preparing and implementing, in accordance with foreseeable threats, plans for the protection of critical infrastructure and maintaining their own back-up systems to ensure their security and sustain their operation until they are fully restored.

PROTECTION PLAN – REQUIREMENTS

The executive act of the cited law is the Regulation of the Council of Ministers of 30 April 2010 on Critical Infrastructure Protection Plans. Its provisions clarify how to establish, update and structure critical infrastructure protection plans to be drawn up by owners and possessors of either stand-alone or dependent critical infrastructure facilities, installations or equipment, hereinafter referred to as 'critical infrastructure operators', and the conditions and procedure for recognising the obligation to have a plan that meets the requirements of a critical infrastructure protection plan.

The regulation specifies, *inter alia*, the elements that should be included in the plan, and these are, in order:

1) general data, including but not limited to: name and location of critical infrastructure, its operator and the entity managing the undertaking on behalf of the operator, the data of the persons responsible for maintaining contacts with relevant entities on critical infrastructure protection and the person drawing up the plan.
2) data on critical infrastructure covering inter alia, the characteristics and basic technical parameters, a plan (map) showing the location of the facilities, installation or system, and the functional connections to other facilities, installations, equipment or services.
3) characterisation of, inter alia: threats to critical infrastructure and assessment of the risk of their occurrence together with foreseeable scenarios for the development of events, and the dependency of critical infrastructure on other critical infrastructure systems and the potential for it to be disrupted by interference with other critical infrastructure systems, its own resources that may be used for the protection of critical infrastructure, and resources of relevant territorial authorities that may be used for the protection of critical infrastructure.
4) essential options include, but are not limited to: acting in the event of a threat or disruption to critical infrastructure, ensuring the continuity of critical infrastructure, and restoring it.
5) principles of cooperation with locally competent: crisis management centres, and public administration bodies.

Pursuant to the CM Act, the Director of the Government Security Centre shall: draw up, on the basis of the detailed criteria referred to in paragraph 2(3), in cooperation with the relevant ministers responsible for the systems, a uniform list of facilities, installations, equipment and services comprising critical infrastructure by system. The list also distinguishes between Critical Infrastructure located in the territory of the Republic of Poland and European Critical Infrastructures located in the territory of other Member States of the European Union that may have a significant impact on the Republic of Poland. The list is classified. The statutory obligation is reflected in Annex 2 to the National Programme for the Protection of Critical Infrastructure (2020 text, 'RESTRICTED' clause – 'Annex 2 to the National Programme for the Protection of Critical Infrastructure – Criteria for distinguishing facilities, installations, equipment and services that are part of critical infrastructure systems – consolidated text'. The operator of critical infrastructure shall draw up the plan within 9 months from the date of receipt of information from the Director of the Government Security Centre on the inclusion of the development in the list of the above facilities.

The plan according to the Regulation is agreed with (as far as they are concerned with the territorially competent):

1) The Voivode,
2) The Regional Commander of the State Fire Service,
3) The Regional Police Commander,
4) The Director of the regional water board,
5) The voivodeship building inspector,
6) The voivodeship veterinarian,
7) The State Regional Health Inspector,
8) The Director of the maritime authority,
9) and with the Minister for Climate and the Environment.

Coordination takes place by signing the coordination form with the above within 14 days of receiving the plan (except for the Minister for Climate and the Environment, who should sign the sheet within 45 days of submitting the plan). The Critical Infrastructure (CI) Operator may be refused agreement to the plan either in whole or in part, and this may occur in the case of: presenting solutions that do not guarantee the security of critical infrastructure or inconsistency with the National Programme for Critical Infrastructure Protection. The Director of the Centre, after considering any discrepancies (the CI Operator submits the plan together with a protocol of discrepancies for approval to the Director of the Centre within 14 days from the date of completion of agreements with all entities), approves the plan within 90 days from the date of submission. It should also be noted that plans should be updated as necessary, but at least once every two years.

RISK MANAGEMENT

Another key aspect (if only in terms of cyberattacks on the Ukrainian energy sector or a wind power operator in Germany), is the provision of ICT security. Article 6.1.5 b of the CMA applies to operators of CI (owners, sole and dependent holders), who are also operators of key services (the Act of 5 July 2018 on the national cyber security system specifies from operators of

key services, as companies and institutions providing services that are vital to sustaining critical social or economic activity. Such operators include representatives of the energy sector). This Article mandates that critical infrastructure protection plans include documentation on the cybersecurity of the IT systems used to provide critical services.

The most crucial thing for operators in the near term is to consciously select an experienced entity to carry out this key task, develop procedures, define a set of possible threats to critical infrastructure, and provide an assessment of the risk of their occurrence together with anticipated scenarios for the development of events, and implement appropriate technical protection for the facilities.

Guidance on how to properly implement CI protection can be found in the "National Programme for the Protection of Critical Infrastructure" published by the Government Security Centre in 2020 – “Standards to ensure the smooth functioning of critical infrastructure – best practices and recommendations”.

This document provides basic information on the technical and organisational aspects of critical infrastructure protection. It can be used as a set of specific guidelines for the construction and operation of a CI protection system. In addition, the document offers an assessment of the effectiveness of the various safety assurance methods, as well as a proposal for an implementation strategy to ensure that it is most effective.

It is crucial to treat critical infrastructure protection as an interdisciplinary issue. Regardless of which types of protection are chosen and implemented in an organisation, four elements are important in the implementation of all types:

1) conducting educational activities,
2) appropriate organisational structure of the safety management division,
3) choice of implementation strategy,
4) verification of the solutions adopted and their updating.

One of the primary principles contained in the above document is that of proportionality and risk-based action. This implies that any action taken to ensure the protection of CI should be proportionate to the level of risk of disruption. This applies to both the CI protection model adopted, the types of CI protection, and the forces and resources used. From the point of view of the Programme, this is a key element, determining and justifying the actions taken to reduce the risk of CI disruption.

The risk assessment should be the basis for setting standards for the protection of CI and prioritising actions. Before embarking on any risk-related analysis (the impact of uncertainty on the goal), there are two issues to consider. Firstly, it is important to remember that risk assessment is a complex concept. According to the PN-ISO 31000 standard, risk assessment consists of:

1) identification of risks,
2) risk analysis,
3) risk evaluation.

The recommended way to carry out threat identification, analysis and risk estimation is to carry out the following steps:

1) identification of the processes within the organisation,
2) determination of impacts – identification of critical processes,
3) indication of resources,
4) identification of threats and vulnerabilities,
5) analysing the risks,
6) risk evaluation.

CONCLUSIONS

In summary, the issues of ensuring security in an era of increasing importance of electricity and increased activity by actors linked to the Russian Federation, aiming by their actions to destabilise steady supplies of energy streams and manage fear, coupled with the significant distance of Offshore Wind Farms from ports from which capable and legally authorised services to intervene can operate, are extremely important. The planned production of electricity "from the sea" from 2025 onwards should be preceded by a careful analysis of the risks and safeguards for this key generation sector for the country's energy security and for the decarbonisation of the Polish energy sector. Analyses should be carried out over the next few decades and procedures confronted with the multiplicity of hazards at sea. Risk estimation should take place with specialists from the physical and cyber domains of facility defence, as well as with experts directly familiar with the specifics of maritime operations.