

Damian Szacawa

## **“Soft security” in the Baltic Sea Region: regional cooperation to enhance societal resilience and critical infrastructure protection**

**The Nordic states consider critical infrastructure protection as part of their comprehensive security. The long-standing tradition of trans-border cooperation in this area will facilitate the implementation of the EU’s Critical Entities Resilience (CER) Directive. The exchange of experience and practical operational cooperation within regional structures (Nordic Council of Ministers and Council of Baltic Sea States) also contributes to resilience in the ‘soft security’ areas in the Baltic Sea region.**

**The importance of critical infrastructure in enhancing the resilience of the Nordic states.** The Nordic states perceive the protection of critical infrastructure as an important part of a broader system to strengthen the resilience of society. They have shifted their emphasis from protecting critical infrastructure to building and strengthening its resilience relatively early compared to other European countries. This approach, which is characteristic of the Nordic model, is part of a broad understanding of civil protection and is part of a comprehensive view of security (see more in [“IEŚ Commentaries”, No. 1045](#)). It is based on the concept of total defence and civil defence systems that were built up during the Cold War. The main focus of this approach is on the performance of society and government under all circumstances, rather than protecting individual components of critical infrastructure from extreme events.

The solutions adopted so far by the Nordic EU members differ in the details. The Swedish civil defence model focuses on the local level of resilience. In Denmark, the core emphasis is not on the critical infrastructure itself but on the prevention of the possibility of its malfunction and/or damage and the minimisation of the consequences of such events. Nevertheless, both models follow the 2006 Finnish critical infrastructure protection strategy, which focuses on the need to secure the delivery of vital societal functions rather than protecting the infrastructure itself. This means that resilience is based on prevention, mitigation, and preparation before a crisis occurs as well as the response during a crisis. It also includes post-crisis recovery, for example, in the event of an interruption to a critical service.

A gradual harmonisation of solutions in this area is expected in the coming years as a result of decisions taken within the European Union. On 14 December 2022, the Critical Entities Resilience Directive (CER Directive)<sup>1</sup> and the amendments to the Directive on measures for a high common level of cybersecurity within the Union (NIS 2 Directive)<sup>2</sup> were adopted at the proposal of the European Commission. Both directives entered into force in mid-January 2023 and should be transposed into the national laws of EU Member States by 17 October 2024.

Both documents considerably broadened the understanding of critical infrastructure, allowing the inclusion of the resources of entities operating in eleven sectors, which include energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration, space and food

<sup>1</sup> Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, (Official Journal of the European Union L 333, 27.12.2022), <https://eur-lex.europa.eu/eli/dir/2022/2557/oj>

<sup>2</sup> Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), (Official Journal of the European Union L 333, 27.12.2022), <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

production, and processing and distribution. The European Commission has thus covered key societal functions, critical infrastructure sectors, and Critical Entities in a single document.

**Baltic regional formats as platforms for sharing experiences.** The Nordic states have played an active role in shaping EU policy on critical infrastructure protection. They have cooperated intensively with NATO and EU structures in the second decade of the 21st century in this regard through the exchange of experience and best practices on critical infrastructure protection. The recognition that critical infrastructure resilience needs to be seen as a much broader task than just crisis planning, accompanied by a desire to develop mechanisms for better coordination between the Nordic states, is also constantly present in the work of the regional structures, i.e., the Nordic Council of Ministers (NCM) and the Council of the Baltic Sea States (CBSS). It is worth noting that so far this cooperation has focused on civil protection rather than critical infrastructure resilience.

In Northern Europe, the first framework agreement on rescue services cooperation was concluded in 1989 between Denmark and Norway, while Finland and Sweden joined in 1992 and Iceland in 2001. This cooperation, which includes practical and operational cross-border arrangements, is called Nordred. In connection with this, a number of such regional and local agreements have been concluded between municipalities in Sweden, Finland, Norway, and Denmark. Since 2005, civil protection has been included at a higher level in the areas of NCM cooperation. In practice, this means high-level ministerial or director-general meetings twice a year resulting in joint statements such as the Hague Declaration (The Hague I) of 2009 and the second Hague Declaration (The Hague II) of 2013, issued by the Nordic ministers responsible for civil protection. Both documents addressed the adoption of the same strategic approach towards civil protection across the Nordic region, which has been reflected in practical terms in regular, rotating training in emergency decision-making and improved cross-border crisis management.

Strengthening societal resilience has been one of the major priorities of the CBSS' work in recent years. Finland's presidency (July 2023 – June 2024) has been accompanied by the promotion of the concepts of comprehensive security and enhanced emergency preparedness. Their importance in cross-border cooperation in the CBSS was highlighted in the Porvoo Declaration, which was adopted at the 21st Ministerial Session of the CBSS in June 2024. States in the region have advocated strengthening resilience and crisis preparedness, emphasising the need to strengthen ties between democratic and like-minded states in the region.

This is being followed up by Estonia, which seeks to further enhance resilience in areas of so-called 'soft security'. During its presidency (July 2024 – June 2025), Estonia intends to make use of CBSS structures, including operational cooperation within the Baltic Sea Region Border Services Cooperation (BSRBCC) and the Civil Protection Network (CPN). Increased situational awareness and preparedness for unexpected situations is necessary given the deterioration of the overall security situation of the BSR after Russia's aggression against Ukraine (see more in ["IEŚ Commentaries", No. 875](#)) and after taking into account the impact of major incidents in the region (destruction of parts of three of the four Nord Stream 1 and 2 pipelines, damage to the Balticconnector pipeline). Estonia, under its Presidency, also plans to put more emphasis on issues related to the protection of critical infrastructure in the Baltic Sea basin, the challenges of mass evacuation and sheltering, and the instrumentalization of migration at the eastern borders of the states of the Baltic Sea region. Therefore, through cooperation with the Baltic Sea states, Estonia complements its national civil defence activities (see more in ["IEŚ Commentaries", No. 1179](#)).

## Conclusions

- The Nordic states have been taking steps to ensure the resilience of critical infrastructure for more than fifteen years. The model they have adopted refers to the concept of total defence and is characterised by an extension of the concept of societal resilience. The follow-up to this way of thinking is a shift from the protection of critical infrastructure facilities to resilience-improving activities, combined with the inclusion of a variety of actors and the coordination of activities across multiple sectors.

- The Nordic model, adapted to the specific needs and capabilities of individual states, is evolving as the security environment changes. The risk of damage to critical infrastructure systems is no longer just a potential hybrid threat, but a real possibility to disrupt services critical to the functioning of society. Therefore, greater emphasis must be placed not only on enhancing the resilience of critical entities but also on the physical and cyber protection of critical infrastructure. At the same time, the applicability of Nordic solutions in other BSR and Central European countries requires their adaptation to local circumstances. They must take into account a number of variables, including but not limited to existing social and political structures and legal arrangements.
- The CBSS's expert groups and networks provide a good platform for the exchange of experience between specialists/experts and politicians from the countries in the region. Responding to practical needs, they contribute added value to regional cooperation and enhance resilience in areas of soft security, especially in the context of the coordination of cross-border activities, exchange of best practices, and improved risk management.