

# APPLICABLE FOREIGN PRACTICES: LEARNING FROM FINLAND, UKRAINE AND THE NORTH SEA

Create Lithuania projects are unique in that they foster and advocate for analyzing and integrating foreign best practices into the project structure. This aspect of the project structure encourages project managers not only to apply their own professional experience gained abroad but to identify and analyze good foreign practices relevant to the project. In this way, the goal is to learn from the success stories abroad and understand what foreign practices or models can be tailored or adapted to improve any identified bottlenecks within the project or serve as a benchmark to inspire a positive change in Lithuania.

## Foreign Best Practices: Looking North

In different areas, varying from economic governance, innovation to societal development, Lithuania looks to some Nordic countries as an example, recognizing that there are areas still requiring growth to reach that level and tailoring already existing good practices to fit Lithuania's reality. This is reflected on the [strategic level](#), [regional level](#), and public statements by key [ministries](#) and [institutions](#). Now, with growing [Europe-wide attention to resilience building in the energy sector](#), mainly driven by Russia's exploitation of energy security as a tool of war and pressure, as well as an increase in sabotage attacks on critical offshore and onshore infrastructure, Nordic examples once again prove highly relevant.

Finland as a frontline states with a large territory and long border with Russia, is [unique for its total defense approach](#), characterized by close cooperation between military, civil society, and the private sector to ensure national resilience. Despite their high readiness, [the Nordic countries are revising](#) their strategies, laws, and cooperation frameworks to counter hybrid threats and closing legal and institutional gaps between peacetime emergencies and war. As the increasingly deteriorating Euro-Atlantic security environment demands adaptation, Finland offers a leading example, with many of their reforms and long standing solutions applicable [elsewhere in the region and across the EU](#).

## Case study: Finish Best Practices in Building Resilience in the Energy Sector

### Finish Comprehensive Security Model

Within the Nordic countries, the [Finnish model](#) stands out for its unique and long-established comprehensive security model, which has evolved from the traditional total defense approach and is [built around sector-specific cooperation between ministries, public authorities, businesses and industry leaders](#)<sup>1</sup>, outlined in Finland's [Security Strategy for Society](#). While the total defense approach primarily focuses on preparing for war and military operations through close public-private cooperation, [the comprehensive security model broadens this scope](#) to tackle modern challenges such as hybrid threats and cyberattacks, adopting an "all-hazards" approach. This expanded approach is particularly relevant to energy security, where protecting critical energy infrastructure requires coordinated efforts across

---

<sup>1</sup> Public authorities within the Finnish context refers to government bodies and agencies at the national and regional levels, including ministries, regulatory agencies, emergency services, and sometimes municipal authorities.

government, public sector, businesses, industry<sup>2</sup>, and civil society to ensure resilience against both traditional and emerging threats.

### **Finland's NESAs and Importance of Public-Private Cooperation**

A central element of the Finnish comprehensive security model is the creation of collaborative industry groups focused on operational preparedness and resilience. The model highlights the strategic [importance of public-private partnerships and voluntary private sector participation](#). A distinctive feature of the Finnish system is the close public-private collaboration coordinated by the internationally unique public agency [National Emergency Supply Agency \(NESA\)](#), an organization operating under the Ministry of Economic Affairs and Employment of Finland, with objectives set by the [Finnish Government](#). The primary [objective](#) of NESA's security of supply policy is to ensure that major disruptions and emergencies can be managed through national measures, enabling the functioning of critical infrastructure<sup>3</sup>, production, and services to meet the essential needs of the population, the economy, and national defense.

At its core is the [National Emergency Supply Organization \(NESO\)](#), a network [supported and guided by NESA](#). The NESO manages 23 cooperative committees, called "pools", across seven sectors<sup>4</sup>, focusing on [joint activities such as](#) situational awareness, training, and sharing of best practices. The [NESO network pools are managed by business operators](#) who oversee operational preparedness within their sectors. The added value of the [industry-led approach in the pool system is that the PPP-framework](#) is evaluated as a more dynamic approach rather than as a detailed regulation by authorities. It allows relevant stakeholders to gain the required skills and exchange knowledge without bringing too much burdensome bureaucracy upon them. This cooperation format provides the industry with the support needed for the practical implementation of the majority of the preparedness efforts, while the ministries responsible are expected to manage, supervise and coordinate preparedness-related activities in their respective sectors.

Historically, [NESO focused](#) on managing physical resources and emergency stockpiles (energy, medical supplies, food), ensuring their availability during crises. However, as the threat landscape evolves, the role of NESO's pools [has broadened beyond material stockpiling](#) to emphasize the [resilience, operational continuity, and cybersecurity](#) of [critical infrastructure](#).

"The security of supply of Finland is built together with the private and the public sector, and it requires seamless cooperation. Society has no backup system that could replace the operators critical to security of supply. Therefore, it is important that companies have good continuity management, and NESA supports this in its work," [says Janne Känkänen, CEO of NESA](#).

Regular meetings within these sectoral cooperation groups further strengthen coordination, communication, and continuity across different key actors for the country's resilience and preparedness.

---

<sup>2</sup> In this context industry is as the broader sector made up of many businesses working on similar type of product or service. Businesses and industry leaders refer to both individual companies and the key players or representatives across the whole sector.

<sup>3</sup> Critical infrastructure [means](#) the basic structures, services and related functions that are essential for maintaining the vital functions of society. These include the electrical grid, the water supply, transport routes and secure connections for data communications and financial transactions.

<sup>4</sup> Seven vital functional areas to be secured include leadership, national defense, internal security, economy and infra-structure, the functional capacity of the population and services, international and EU activities, and psychological resilience.

### **Safeguarding energy supply: Industry-specific cooperation**

It is recognized in Finland's National Security Strategy that [the availability of energy affects all functions of society, and disruptions may endanger the critical functions and the wellbeing of the population](#).

Safeguarding Finland's energy supply is a critical national objective overseen by the Ministry of Economic Affairs and Employment (MoEE). The Energy Supply Sector within NESO, encompassing the Power Supply Pool and Oil Pool, coordinates preparedness planning to ensure the continuous procurement, transmission, and distribution of electricity, heat, and gas during emergencies. The sector companies implement the practical measures. Fingrid Oyj, the main grid operator for electricity, and Gasgrid Finland Oy, the transmission network operator for gas, are responsible for the functioning of the transmission systems. The national grid operator Fingrid Oyj coordinates the Energy Supply pool, with other power companies participating in its activities to maintain continuity in all situations. The pool also participates in national preparedness exercises and organizes training for contingency managers.

NESA has also signed power production reservation agreements with companies in the pool. The collaboration with the public authorities has also ensured that the companies in the pools can request special rights for their critical employees to be exempt from military service during crises to ensure business continuity.

Effective collaboration among ministries, sector companies, and agencies like the Energy Authority<sup>5</sup> and the Finnish Safety and Chemicals Agency ensures energy supply resilience, which is critical to society's functioning and well-being.

### **Finland's Efforts to Improve Protection of Critical Infrastructure: Strengthening Domestic Capabilities and International Cooperation**

Despite being known as one of the countries setting an example in preparedness and crisis response by effectively reacting to evolving security threats, Finland has undertaken significant reforms to enhance the protection and resilience of critical infrastructure. Legislative changes include a comprehensive reform of the Emergency Powers Act aimed at strengthening material preparedness.

In response to the EU Critical Entities Resilience (CER) Directive a general act on protecting critical infrastructure led by the Ministry of the Interior, [is under preparation](#) and aims to define shared requirements, roles, and responsibilities for authorities and private actors. The act transposes the CER Directive (Critical Entities Resilience Directive) into national law and [has entered into force on the 1<sup>st</sup> of July 2025](#). Ministries will be tasked with identifying critical entities within their sectors. Identified critical entities will face obligations such as conducting risk assessments, developing resilience plans, and ensuring operational continuity under emergency conditions. Additionally, supervisory authorities will be appointed from the administrative branches of the ministries and companies providing vital services.

Security clearance procedures are also being tightened. The Ministry of Justice proposed [extending the Security Clearance Act](#) to cover personnel with access to sensitive information at critical sites, including personnel related to the maintenance of the infrastructure critical for the functioning of society, such as energy. Simultaneously, [NESA's role continues to evolve](#) through reviews and recommendations for [improving even further the public-private cooperation](#) in the sphere of security of supply.

Recognizing the importance of [international interdependencies](#), Finland is also deepening cross-border and international cooperation. Notably, it is strengthening preparedness ties with Sweden and other [like-minded partners](#), including Australia, Canada, Japan, and South Korea. Finland's cooperation with

---

<sup>5</sup> The Finnish Energy Authority (Finnish: Energiavirasto) is an expert authority within the Ministry of Economic Affairs and Employment in Finland.

Estonia focused on [protecting underwater energy transmission connections](#) has also intensified in the past years. In addition, Finland is hosting the European Centre of Excellence for Countering Hybrid Threats (Hybrid COE) known for its capabilities in addressing emerging hybrid threats, providing relevant trainings and research aimed at supporting all the center's member states, and raising the general awareness on the topic of the hybrid threats. Therefore, Finland is uniquely positioned to contribute and support joint training, research, and information sharing on hybrid threats, on both NATO and EU levels.

### **Overall Recommendation:**

Finland demonstrates how deep institutionalization of resilience, backed by cross-sector cooperation and strategic use of international mechanisms, creates a robust energy security posture. Lithuania can adopt these learnings by:

- Institutionalizing public–private “pool” frameworks.
- Embedding private sector into planning via regulatory structures.
- Focus on/Enhance cross boarder cooperation for the shared critical infrastructure resilience measures!
- Strategically leveraging EU and NATO tools to supplement national capacity.
- More on Finland's comprehensive security model can be found here [Secretariat – Turvallisuuksomitea](#)

## **Best Practices from the North Sea: What the Baltic Region Can Learn about Protecting Energy Infrastructure**

### **Introduction: A Shared Challenge Across Two Seas**

Across both the North Sea and the Baltic Sea, the threat to critical undersea infrastructure has emerged as one of the most pressing security issues of the region. From power and data cables to offshore wind platforms and oil and gas pipelines, these assets sit vulnerable on the seabed, exposed to the increasingly aggressive probing of state actors. Russia, in particular, has taken a keen interest in mapping and observing European undersea infrastructure. In this evolving threat environment, countries bordering the North Sea have taken several meaningful steps that offer valuable lessons for the Baltic Sea region.

This section explores how the North Sea countries have approached the protection of their energy infrastructure and makes the case that the North Sea is not only keeping pace with the Baltic, but in several ways, has taken earlier and more operationally significant steps. By looking at how countries around the North Sea have collaborated, responded to threats, and built tools to share information, this section identifies best practices that could enhance Baltic energy security moving forward.

### **Building Political Coordination: The North Sea Joint Declaration**

In early 2024, six North Sea countries, Belgium, Denmark, Germany, the Netherlands, Norway, and the United Kingdom, signed a joint declaration aimed at protecting critical offshore and undersea infrastructure. Officially titled the "[Joint Declaration on Cooperation Regarding Protection of Infrastructure in the North Sea](#)," the agreement emerged from the 2023 North Sea Summit in Ostend, Belgium. The timing of this declaration is important: it was signed more than a year before a similar Baltic Sea agreement.

The North Sea declaration is not a legally binding treaty but rather a shared commitment to pursue joint protective measures. It outlines the following steps:

- Cooperate in strengthening the resilience of undersea infrastructure.
- Take national actions to safeguard critical energy and communication assets.
- Create joint working groups composed of national authorities.
- Set up a central contact point for coordination and rapid communication.
- Develop shared working plans and agree on information-sharing protocols.

Though its legal standing is limited, the declaration has already catalyzed real-world action and regional cooperation. For example, the [development of the NorthSeal Platform](#), [Dutch investments into the deployment of surveillance systems](#), and [a British-Norwegian partnership focused on protecting subsea infrastructure](#) all reflect a common understanding among participating states that energy infrastructure is both a shared vulnerability and a shared responsibility.

### **The Baltic Sea Memorandum: Similar in Aim, Later in Action**

In May 2025, the Baltic countries followed suit with their own Memorandum of Understanding (MoU) on protecting undersea critical infrastructure. Signed in Vihula, Estonia, the Baltic MoU included a wider range of participants including Denmark, Estonia, Finland, Germany, Iceland, Latvia, Lithuania, Norway, Poland, Sweden, and the European Union. It lays out a more detailed and structured format for cooperation, including the creation of an expert group, joint reviews of national security measures, and efforts to explore technological innovations.

However, while more expansive on paper, the Baltic MoU is still in its early stages of implementation. At the time of writing, it has yet to generate an operational platform or coordinated actions akin to what has emerged in the North Sea. This difference between political will and operational capability is key: while the Baltic has created a stronger framework, the North Sea has already moved toward implementation.

### **A Functional Model: The NorthSeal Platform**

One of the most important innovations to emerge from the North Sea cooperation is the [NorthSeal platform](#), developed by Belgian Secure Communications, the new secure communications system of the Belgian government. Designed as a secure digital infrastructure for cross-border information exchange, NorthSeal enables the rapid sharing of data, real-time monitoring of suspicious maritime activity, and integration with NATO threat intelligence. It represents a tangible leap from policy agreement to operational readiness.

NorthSeal [functions as a centralized hub](#) where participating countries can communicate about potential risks to undersea cables, wind farms, and other infrastructure. It has already facilitated better maritime domain awareness, helping countries track in real time potentially hostile vessels operating under the guise of commercial or fishing ships, or those with their identification systems deactivated. NorthSeal's information-sharing link with NATO strengthens the alliance's intelligence-gathering efforts and broadens the strategic capabilities of both allied navies and Allied Maritime Command (MARCOM).

No similar platform currently exists for the Baltic Sea. The Baltic MoU discusses coordination and knowledge exchange but has yet to materialize into a tool or system for real-time, secure communication focused on protecting critical undersea infrastructure. Developing or adopting a similar platform should be a priority for the region.

## Understanding the Threat: Mapping and Probing Activities

A major driver behind the North Sea coordination has been the increasingly visible activity of Russian naval and intelligence units. Investigative reporting and intelligence leaks have revealed that [Russia has undertaken extensive mapping of undersea infrastructure](#) throughout the North Sea. Using ships disguised as fishing vessels or civilian craft, and utilizing legal challenges post by the UN Convention on the Law of the Sea (UNCLOS), as well as [submarines operating in international waters](#), Russian operatives have been able to surveil cables, pipelines, and energy platforms with little legal recourse from affected countries. Some notable examples include the presence of heavily armed Russian “research vessels” [performing intelligence operations under the guise of civilian activity](#).

Some estimates suggest that [up to 1,000 espionage incidents](#) have taken place in the North Sea alone. While no confirmed acts of sabotage have occurred in the region, the scale and persistence of these incursions have heightened the sense of urgency among policymakers. A [2023 joint media investigation into Russian spy ships](#) operating in the North Sea reinforced the view that the threat is not theoretical, but active and persistent.

This shared recognition of threat has enabled North Sea countries to treat undersea energy and communications infrastructure protection not as a secondary concern but as a central pillar of national and regional security.

## Implications for the Baltic Sea Region

For countries like Lithuania and the other Baltic states, the North Sea experience provides a roadmap for how early coordination and practical implementation can increase regional resilience. The Baltic states have already demonstrated strong political commitment to coordinating the protection of undersea infrastructure, but they now face the challenge of moving from policy to practice.

Key lessons include:

- **Move Quickly from Agreement to Action:** The North Sea Joint Declaration may be less detailed than the Baltic MoU, but it spurred the rapid development of tools and working groups. The Baltic region should not delay operationalizing its agreement.
- **Invest in Shared Platforms:** A centralized information-sharing and threat-monitoring system akin to NorthSeal would significantly enhance the Baltic region's ability to detect and respond to threats.
- **Foster Maritime Domain Awareness:** Espionage and probing often occur under legal grey areas of international maritime law. Joint surveillance, shared intelligence, and public awareness are crucial tools in addressing these challenges. Additionally, highlighting these legal issues in international arenas will contribute to the discussion around amending these laws to benefit security.
- **Include NATO and the EU:** Just as NorthSeal has integrated with NATO systems, Baltic coordination should ensure alignment with both NATO and EU maritime and cyber defense frameworks and include information sharing and threat tracking to allow for best practice sharing and coordinated responses from allies outside of the Baltic Sea Region.

## Conclusion: The Value of Practical Cooperation

The North Sea region shows that even non-binding political agreements can generate meaningful action when there is shared threat perception and a willingness to innovate and act. While the Baltic states have

made impressive strides with their 2025 Memorandum of Understanding, the experiences of their western neighbors demonstrate the importance of turning policy into practice.

By studying and emulating the North Sea approach, particularly the use of secure communications platforms, early political coordination, and maritime threat awareness, the Baltic region can strengthen its collective resilience against undersea infrastructure threats. The threats are real and growing, but so too is the capacity for regional cooperation to mitigate them.

## Ukraine: Lessons Learned from Real World Experience

Russia's invasion of Ukraine in 2022 has provided valuable lessons that Lithuania's energy security ecosystem can take into account when determining future strategies for their security, especially when it comes to infrastructure protection and security of supply. Ukraine has, for over three years, been repelling attacks that are similar to the ones Lithuania is preparing for. Ukraine has had learned success, and while Russian tactics and strategy inevitably will change to reflect their own learned experiences, lessons for Lithuania can be drawn from these successes and failures.

Ukraine has experienced both unexpected successes and failures in defending their energy systems. For example, from November 2022 to August 2024, Kyiv [did not experience](#) an unscheduled blackout. However, due to the location of some key energy infrastructure, a portion of generation has been lost. Sources estimate that, as of spring 2024, [around two-thirds of the country's dispatchable power generation](#) has fallen under occupation, which is being coupled with [a systematic attack on the grid network](#).

### Successful Aspects of Ukraine's Wartime Energy Defense

The Ukrainian energy sector's ability to withstand direct attacks from artillery, missiles, sabotage, and other methods designed to disrupt the flow of energy to residents and the military has proven to be a massive asset to the defensive forces. Their ability to maintain energy for both the military and civilians allows military forces to continue to push back Russian advances, maintain societal morale in a long and grueling war, and become a leader for other countries to emulate.

A few natural aspects of the energy system allow for Ukraine's robust security and resilience. First, Ukraine's large size and diverse generation capacity allows for other sectors to carry different needs when necessary. For example, although Russia has primarily targeted thermal power generation and, as of September 2024, Ukraine [had lost 80% of its thermal capacity](#) due to Russian attacks, the nuclear energy sector, which [contributes 55% of total generation](#), has been largely spared. Ukraine's diversification of energy production complicates Russian efforts to effectively destroy the country's energy system.

Ukraine's [size provides another natural defense strength](#). Energy generating capacity in the far west of Ukraine has been spared from the front line fighting that other parts of Ukraine has faced. This limits the number of threats these infrastructure objects need to prepare for. In western Ukraine, infrastructure objects need to be protected from missiles, drones, and sabotage, not direct attacks and artillery. This difference in threat picture allows for more effective defense, which, in turn, allows for more consistent generation ability.

Additionally, Ukraine developed a strong and flexible distribution system. While Russia has been attacking the transmission system, it has so far spared large parts of the distribution system. Ukraine has done well to build cables and distribution infrastructure that [can distribute more than the regular capacity](#). This extra capacity allows for flexibility in responding to outages elsewhere in the system.

The most successful aspect of Ukraine's defense of energy systems is its ability to complete timely and effective repairs that keep the energy system functioning with minimal disruption. The brave repair teams around Ukraine and [heroic individual efforts](#) have neutralized some of the Russian targeting of energy systems by [performing repairs within days, and sometimes hours, of destruction](#). Ukraine's ability to keep infrastructure in working order and maintaining operation of generation plants throughout the country, even [occasionally during missile and drone attacks](#), has allowed Ukraine to continue its resistance.

Ukraine's ability to perform repairs and maintain generation is complimented by its international partners. International partners, including Lithuania, [have provided spare parts, repair knowledge, and infrastructure upgrades](#) that have been vital to maintaining Ukrainian energy resilience. Without donations from [international partners](#), Ukraine's ability to provide timely repairs would not have been possible, which would further compromise its ability to defend itself.

Additionally, Ukraine's introduction into ENTSO-E (the European Network of Transmission System Operators for Electricity) was a significant step in the security of its energy network. Before the full-scale invasion in 2022, Ukraine had been preparing to synchronize its electricity grid with the European network, through ENTSO-E. Following the invasion, this emergency synchronization was implemented ahead of schedule to ensure stability and independence from the Russian grid. Synchronization allows for Ukraine to [manage its transmission network more freely and autonomously](#). More importantly, introduction into ENTSO-E allowed Ukraine to ["desynchronize from the Russian controlled IPS/UPS synchronous zone"](#), which was providing Russia with critical intelligence about Ukraine's electricity system.

### **Unsolved Vulnerabilities in Ukrainian Energy Security**

While Ukraine has a strong and effective energy security ecosystem, there are still some vulnerabilities that prevent complete energy security. These vulnerabilities are typically difficult to fix, especially because wartime conditions prevent new large scale construction projects and infrastructure upgrades.

The main vulnerability of Ukraine's energy sector is its [reliance on fixed, high-value infrastructure](#), such as power plants and transformers. Large and difficult to defend infrastructure objects present target opportunities for Russian missiles and drones. Ukraine is actively deploying microgrids and decentralized energy systems as a key lesson from wartime infrastructure damage. These technologies have become central to maintaining resilience in the face of persistent attacks. While modularity and mobility will be important for coming projects, some types of energy infrastructure cannot be designed with much modularity and mobility in mind. To counteract this, Ukrainians have been providing as much air defense and physical protection as possible, being forced to move scarce and critical systems from the front lines to defend infrastructure.

Elaborating on this, [the scarcity of air defense resources adds to the vulnerabilities](#) of Ukraine's energy security. From the beginning of the full-scale invasion, and even before, Ukraine has requested more air defense systems from its international partners. While international partners have been willing to provide limited numbers of these systems, Russia's ability to outpace the defensive capabilities with offensive drones and missiles has continued to harass Ukraine's energy infrastructure. [Ukraine's inability to consistently meet its air defense need](#), especially regarding energy infrastructure, continues to be a vulnerability that Russia exploits.

### **Russia's Change in Strategy**

During the three years of the Russian invasion of Ukraine, Russia has also changed its strategy. Most notably, during the first few months of the invasion, experts have noted that [Russia intentionally refrained](#)

[from attacking energy infrastructure](#), believing that there was no need. Analysts believe that Russia expected to quickly take the territory, so it did not want to take on the costly and difficult process of rebuilding infrastructure it had only recently destroyed. This however changed with Ukrainian resolve and defense. Once it was certain that Ukraine would not be quickly overrun and a long-term war was on the horizon, Russia started targeting energy infrastructure more regularly.

Additionally, with the notable exceptions of the [Chernobyl NPP](#) and [Zaporizhzhia NPP](#), both siezed early in the invasion, and occasional strikes near other facilities, Russia has not systematically targeted nuclear power plants, though repeatedly attacking supporting infrastructure. Fearing the international backlash of targeting such sensitive and fragile infrastructure and risk to the environment, [Russia has generally refrained from direct attacks](#). While this strategy may change in the coming phases of the war, it is important to recognize when planning energy security strategies for the future.

### **Lithuania's Use of Lessons from Ukraine**

While Ukraine and Lithuania differ in their energy systems, threat environments, and resources bases, Ukraine's wartime experience offers specific lessons for strengthening Lithuania's Energy Resilience

For example, Lithuania can follow Ukraine's lead on repair ability. Ukraine's ability to repair and maintain energy systems, even during attacks, is crucial. By stockpiling critical spare parts, designing systems that promote modularity, and focusing on effective training of repair teams, Lithuania can be ready to keep energy flowing even during an invasion. Stockpiling spare parts became crucial to Ukraine's ability to repair systems, and by stockpiling parts before an attack will keep Lithuania from having to find partners to donate those parts in the middle of an attack.

Additionally, promoting modularity and flexibility will allow Lithuania to quickly and easily protect and repair infrastructure. While some objects cannot be designed with a modular function, understanding where modularity and mobility can be utilized will make Lithuania's repair ability even more streamlined, keeping logistical challenges to a minimum.

Finally, promoting effective training of repair teams will be crucial for repair. Ukraine's repair teams work so well because they have been trained on and practiced repairing wartime disruptions. This allows them to quickly and effectively assess damage and provide repairs within the necessary time frames. Developing that capacity will be crucial for Lithuania's ability to withstand any attack.

Table: Applicable Foreign Best Practices

Country/Region	Foreign Practice	Mechanism	Adaptation Potential for Lithuania
Finland	NESA's "Energy Pool"	Industry-led coordination, drills, and readiness plans	Can be piloted within Lithuania's TSO and energy sector actors. Use existing coordination bodies such as National Crisis Management Center as base to kick off a public-private cooperation format.
Finland	NESO's cooperative committees	Multi-sector PPPs for critical infrastructure protection and operational continuity	Structure similar public-private preparedness platforms, especially in energy and ICT. To blend government oversight with private-sector participation and invaluable expertise.
Finland	Institutionalized public-private partnership model	Finland's NESA stands out internationally for its institutionalized public-private partnership model that combines governmental oversight with active private sector involvement in securing critical supplies. In the energy sector, it acts as a linchpin (core actor) ensuring that both public safety and economic continuity are maintained through strategic collaboration, planning, and operational coordination.	Lithuania could strengthen its energy security by adapting Finland's NESA model within its existing structures—coordinated, for example, by the Central Project Management Agency (CPVA) or the National Crisis Management Centre. While Lithuania already has active PPPs and strong state-regulated energy operators, a dedicated coordination unit could institutionalize long-term public-private collaboration for critical supply resilience, planning, and rapid crisis response.
Finland	Hybrid CoE expert pool model	Voluntary national experts, pooled across borders	Could be applied in Lithuania's NATO ENSEC COE; Lithuania could submit RFS for developing a Baltic(+)-wide shared expert database that could potentially be used for any crisis time information sharing as well.

Finland	Legislative reforms	New clearance requirements and CI protection laws	Explore similar updates for infrastructure and critical personnel legislation (e.g., security clearances or background checks and exemption from military service).
Finland	Cross-border preparedness (e.g., with Estonia)	Joint protection of critical assets	Extend and deepen existing cooperation on subsea, cyber, and energy systems (critical cross-border energy infrastructure).
North Sea	Information sharing with international allies	Centralized information gathering and sharing system for North Sea (NorthSeal)	Development of real-time intelligence and information gathering and communication systems for offshore vulnerabilities for the Baltic Sea
Ukraine	Repair Ability	Specialized repair teams for critical equipment	Development of small, effective emergency repair teams to handle any incidents
Ukraine	Repair Ability	Spare parts stockpiling for quick repairs of critical equipment	Identification, storage, and usage of spare parts that are difficult to acquire or produce, allowing for quick repairs to be made to critical equipment
Ukraine	Repair Ability	Effective training of repair teams	Identification, training, and repeated practice of crisis scenarios for repair teams of critical equipment will enhance Lithuania's ability to withstand an emergency
Ukraine	Critical Infrastructure Construction	Promoting modularity and flexibility when designing and building critical equipment	Understanding where modularity and mobility can be integrated into existing and new equipment will enhance both Lithuania's repair ability and protection ability.