Lessons Learned from Coherent Resilience Tabletop Exercises in the Baltic Region

Vytis Kopustinskas[a*], Evaldas Dirginčius[b], Charles Lynn[c], Isabel Asensio Bermejo[a], Lawrence Walzer[c], Darius Aukščionis[b], Hrvoje Foretić[d]
[a]European Commission, Joint Research Centre (JRC), Ispra, Italy
[b]NATO Energy Security Centre of Excellence, Vilnius, Lithuania
[c]Energy Academic Group, Naval Postgraduate School, Monterey, USA
[d]European Commission, Joint Research Centre (JRC), Petten, Netherlands

Abstract: Current geopolitical environment in the Baltic Sea region requires continuous actions to build and enhance resilience of energy infrastructure. Tabletop Exercise proved to be an important tool that can bring together all the stakeholders and foster resilience through cooperation, sharing and networking of neighboring states or regions. A Tabletop Exercise is a facilitated discussion-based exercise conducted in a stress free environment. The NATO Energy Security Centre of Excellence (NATO ENSEC COE) and the Joint Research Centre of the European Commission (JRC) have jointly organised three tabletop exercises in the Baltic region addressing resilience and energy security. The exercises were conducted every two years in 2019, 2021 and 2023. All three exercises were evaluated by a team from Naval Postgraduate School (NPS). This paper presents three tabletop exercises and their major outcomes.

Keywords: Tabletop exercise, Critical energy infrastructure protection, Resilience, Security of supply.

1. INTRODUCTION

A tabletop exercise (TTX) is an informal, discussion-based exercise in which a team discusses their roles and responses during an emergency or crisis, considering several examples of potentially risky situations. The atmosphere is collegial and exploratory, and is not meant to put participants in the mindset they'd have during a real crisis event. Tabletop exercises are used to prepare for crises, with primary aim to identify gaps in legislation and share best practices among the participants [1].

A TTX is in particular useful tool to discuss and prepare for crisis events that might affect several countries having different legal, governance and emergency response systems that need to interact and work together in case of real event. TTX not only serves as a perfect networking event, it could also serve to spark and set up intergovernmental agreements for common crisis response.

Coherent Resilience (CORE) is a series of national and regional level tabletop exercises (TTXs) aimed at enhancing resilience of energy systems in an era of hybrid threats. CORE TTXs have been conducted in Ukraine as well as national and regional programs in the Baltic States and other countries.

The main objective of this study is to provide an overview of the three exercises completed in the Baltic Sea region in the period of 2019-2023 and evaluate their importance and effect in increasing resilience and energy security in the region. As the main focus of the exercises is to improve resilience of energy systems, resilience is understood as system's ability to withstand external shocks and continue to provide services as long as possible, see more details in [2].

2. CORE19 TABLETOP EXERCISE

Coherent Resilience 2019 (CORE 19) was a Tabletop Exercise on the Baltic States and hybrid threats related to regional natural gas supplies and critical energy infrastructure protection. The TTX took place 14-16 May 2019 in Vilnius, Lithuania. The goal of the exercise was to support the national authorities and natural gas transmission system operators (TSO) of the Baltic States in ensuring supply of gas to consumers and mitigating the disruption over the Baltic region. This three-day regional, multilateral, interagency, and public-private sector event was divided into three phases including an academic seminar, a two-day TTX, and a distinguished visitors' day that included after-action briefings. The event brought together 108

participants from 14 NATO and European Union countries, who came from 35 different organisations representing gas supply and energy security stakeholders.

2.1. Scope and Objectives

The goal of the exercise was to support national authorities and gas transmission system operators of the Baltic States in ensuring supply of gas to consumers and mitigating the disruption over the Baltic region through the execution of a tabletop exercise, where national emergency response plans and regional cooperation were exercised. Particular attention was given to the topic solidarity agreements that are required by the EU Regulation 2017/1938.
The target audience for the event included: energy related ministries, gas transmission system operators, crisis management officers, energy (gas) traders and distributors, main gas consumers, market regulators and national Computer Emergency Response Teams (CERTs) of the Baltic States – Lithuania, Latvia, Estonia and Poland and Finland. In total, five EU Member States were active participants of the exercise.

The exercise was conducted in the light of hybrid threats that formed background for the scenario development. This includes not only the major component of security of natural gas supply in a form of supply disruption, but also a mixture of socioeconomic, geopolitical, strategic communication elements to be considered. The starting time of the exercise is selected to be January 25 of year 20YY. The duration of the crisis during the exercise is 14 days. For this time frame two infrastructure situations were exercised: 2019 current situation and future 2020+ situation. The scenario used to conduct the TTX was discussed and finalised during the scenario development workshop on March 5-6, 2019 in Vilnius. It was also commented during Vignettes and injects development workshop on March 27-28, 2019 in Riga.

All the vignettes and injects under developed scenario were discussed during the TTX simultaneously in four syndicates:

a) Solidarity Mechanism of the EU
b) National Preventive Action and Emergency Plans
c) Strategic (Crisis) Communications
d) Cyber security

2.2. Main findings

The following key conclusions were identified by the participants:

Tabletop Exercise as a Tool. Participants noted the value of the tabletop exercise as a forum to share best practices, discuss challenges, and review national and regional plans. Having a community of interest to focus on energy security challenges can lead to improvements in resilience of supply and systems through cooperation and communications. CORE 19 participants could see a continuous cycle of annual exercises, where this event is followed organisation, interagency, national, and again a regional-level exercise.

Future Infrastructure as a Positive Change. Planned future additions to regional energy infrastructure - as identified in the scenario 2020+ – was identified as having a significant positive effect on regional and state energy security. It was very clear to the participants that additional infrastructure would significantly lower chances for solidarity request situations. Such solidarity needs are rather low even with today's infrastructure as it became evident during the exercise. Nonetheless, it was also clear that additional work is required in all areas as it is imperative to further improve resilience.

Cyber Security Remains a Challenge. While tremendous gains have been made in cyber security, experts participating in CORE 19 acknowledged that such security is not yet mature and that energy supplies remain at risk due to current vulnerabilities. Many in attendance further highlighted the importance of ensuring manual operating capability – where practical – be maintained in the event automated systems are catastrophically hacked.

Consider Establishment of Regional Crisis Centers. Given current vulnerabilities in energy security and regional threats, the potential value of establishing Regional Crisis Centres was noted by several technical experts. Participants noted that without a dedicated entity able to view regional atmospherics from such a

vantage point, developing campaigns by potential adversaries may be missed in a timely manner necessary to most effectively thwart such activities.

Layered Consumer Levels. Regional national plans all contained measures for both protected and non-protected customers. While there remain challenges in cutting supplies to non-protected customers when shortfalls demand, many participants noted that it would be advantageous to further delineate the two categories into several in order to best facilitate cutting supply and returning supply to customers in a manner that best mitigates challenges and enables a return to normalcy following such events.

Superior Technical Expertise of Regional Gas Suppliers. CORE 19 indeed brought together an array of technical experts from the Baltic and partner states, who represented gas suppliers, regulators, and numerous organisations with cognisance over national and regional energy security matters. It is clear that regional governments and populations are well-represented by these experienced professionals, who gathered at this event in an effort to share best practices and discuss mutual challenges. The many lessons learned during this event by each of the participants are sure to be brought back to their respective organisations and acted upon in an effort to facilitate continued improvements in regional and national energy security/resilience – continue to support these professionals.

A number of key takeaways was identified by each of 4 syndicates and these are provided in the corresponding sections of the final exercise report [3].

3. CORE21-B TABLETOP EXERCISE

Coherent Resilience 2021 – Baltic (CORE 21-B) was a Tabletop Exercise on the Baltic States and hybrid threats to the regional electric grid with a focus on critical energy infrastructure protection. The TTX took place 20-24 September 2021 in Vilnius, Lithuania. The aim of the exercise was to support the national authorities and electricity system operators of the Baltic States in ensuring supply of electricity to civilian and military consumers and mitigating the possible disruption in the light of hybrid threats over the Baltic region due to vulnerabilities caused by close proximity of unsafe Belarusian Nuclear Power Plant (NPP) and the process of synchronization of the Baltic States power grid with the Continental Europe grid. CORE 21-B was a five-day regional, multilateral, interagency, and public-private sector event that was executed with an academic seminar, a three-day TTX, and a distinguished visitors' day that included after-action briefings. The event brought together over 100 participants from 12 NATO and European Union countries or partner nations, who came from 35 different organizations representing electricity supply and energy security stakeholders.

3.1. Scope and Objectives

The CORE 21-B TTX was prepared in a series of preparatory meetings in Vilnius, Lithuania – initial planning conference (15-16 December 2020), main planning conference and vignettes/injects development workshop (25-27 May 2021), and a final coordination conference (8 July 2021). Note that main preparatory work of the exercise took place during pandemic period and travels were very restricted, forcing meetings to be only online. However, the main TTX event took place only in person.

CORE21-B centered on the resilience of electricity supply to the Baltic State consumers during hybrid attack and Baltic electricity grid synchronization to the Continental Europe grid. The main purpose of the exercise was to evaluate plans, policies, and procedures used to build resilience of electricity transmission systems in case of supply distribution due to hybrid attacks. The aim of CORE 21-B was to support national authorities and electricity system operators of the Baltic States in ensuring supply of electricity to civilian and military consumers and mitigating the possible disruption in the light of hybrid threats over the Baltic region due to vulnerabilities caused by close proximity of unsafe Belarusian NPP (also known as Ostrovets, as well as Astravyets NPP) and the process of synchronization of the Baltic States power grid with the Continental Europe grid.

CORE 21-B objectives were:

- Introduce the main (HYBRID and CYBER) hazards and threats on Electricity Infrastructures in the Baltic countries, based on worst case scenario and taking into account the findings of the research study [4] and mitigate them.
- Support the Electricity grid operators of the Baltic countries keeping resiliency of Electricity supply during the desynchronization from BRELL network and synchronization with the Continental Europe network.
- Exercise the Strategic Communication (STRATCOM) as a tool to mitigate hostile propaganda, fake news, create proactive counter-narrative and enforce solidarity of the relevant states on Electricity policy.
- Ready Crises Response authorities to fight with situations caused by HYBRID attacks in electricity sector due to close proximity of unsafe Belarusian NPP and the process of synchronization of the Baltic States electricity network with the Continental Europe.

The training audience, coming mainly from 6 EU Member States – Lithuania, Latvia, Estonia, Poland, Finland and Sweden, discussed four vignettes and a number of injects for each vignette within 4 syndicates:

a) Syndicate 1 – STRATCOM
b) Syndicate 2 – Hybrid-Cyber
c) Syndicate 3 – Crisis Response
d) Syndicate 4 – Synchronization

3.2. Main findings

The following key takeaways and recommendations are those identified by the broader syndicate teams that consisted of facilitators, participants, and evaluators:

There is a need for increased baseload reserve generation. There is a need in the Baltic States to increase baseload generation capacity and not to rely on interconnections only. This need is particularly evident when the Baltic States operate in isolation mode creating situations with load shedding as the only available option. **Recommendation:** Analyze the feasibility of building new baseload generation capacity in the region. Feasibility is dependent on need, cost of power, and public opinion. The type of fuel can be as diverse as practically reasonable, be it nuclear, gas, hydrogen or others. Due to ongoing climate protection regulations, low or zero green house gas (GHG) emission technologies should be analyzed for feasibility.

Early Multinational Cooperation during Hybrid Scenarios would improve resilience. During crisis events, the national emergency response centers combine various stakeholders from the TSO(s), cyber agencies, intelligence agencies, and others to facilitate a coordinated national and/or multinational response. But regulations have not been updated regarding the notification and declaration of incidents for all hybrid attacks. And when events and indicators did not clearly trigger declaration of a crisis event, the lines of communication to share information across states and agencies were inconsistent and would likely lead to information gaps at decision-making levels. When thresholds were not clearly exceeded, most reporting continued via internal channels, further preventing effective national and multinational response. **Recommendations:** To improve pre-crisis resiliency, establish reporting channels and procedures for TSOs to collaborate amongst themselves regarding events which do not rise to national emergency or crisis levels. Low-level, cross-agency and cross-nation information sharing will permit the Baltic states and their allies to identify potential attacks more rapidly and respond more precisely, neutralizing single aspects in isolation (where possible). The channels should be exercised during multinational exercises at ministry and TSO levels. Pre-crisis resiliency also depends on the level of uncertainty regarding the functioning of the Belarusian NPP that was built in close proximity to the Baltic States in violation of the international nuclear and environmental safety requirements. The high level of uncertainty stemming from low safety standards and secrecy around the Belarusian NPP could motivate adversary to include a nuclear energy aspect in the hybrid attacks expecting that it will act as a strong force multiplier. In order to diminish the hybrid threat potential, the Baltic States and their allies should continue their multilateral and bilateral efforts with the aim to ensure that Belarus implements the highest international nuclear safety standards and strictly follows the principles of openness and transparency. In order to improve preparedness and response, it is important to increase awareness on how to deal with the situations when a nuclear element is used as a part of a hybrid activity toolbox.

Need to evaluate and update prevailing current approach to risk analysis and assessment used by institutions/companies for crisis prevention and mitigation. The current approach still mainly relies on historic evidence/past incidents, and therefore cannot provide adequate preparedness/relevant emergency response mechanisms in situations when adversary employs creative and innovative combinations of different tools with cascading effects in multiple domains in order to achieve its targets and strategic goals. CORE 21-B scenario included a variety of innovative means, including the Belarusian NPP- related toolbox, used by adversary to harm the synchronization process of the Baltic States with the Continental European Network and to coax the Baltic States into continuing market flows of electricity from Belarus. The TTX revealed a number of gaps in current state of crisis preparedness, especially concerning hybrid threats and intentional attacks. **Recommendation:** Include contemporary hybrid threats in risk analysis/assessment methodology as an instrument for crisis prevention and development of mitigation measures.

Developing Alternative Communication Pathways would facilitate more effective, efficient, and timely coordinated responses to crisis situations. The Baltic States display a robust communication capability with their citizens, but it is reliant upon modern telecommunications infrastructure. During lengthy emergencies there was uncertainty about how they would be able to communicate effectively with their citizens. Some syndicate members mentioned having the communications handled at the municipality or city level, but they were unsure what communication pathways were available at those levels. **Recommendations:** 1) Develop an Emergency Broadcast Radio Service that utilizes emergency generator powered transmitters. This system would enable resilience in information dissemination systems for varying types of emergencies. 2) Investigate national cell phone push-notification system as a conduit for emergency information. 3) Investigate commercial off the shelf (COTS) technology for enabling cell phones to access radio broadcasts. 4) Develop protocol for utilizing police car speakers, military PSYOP equipment (speakers and leaflets), and similar equipment as information distribution mechanisms.

Improving emergency cooperation agreements would improve responsiveness and coordination of mutual assistance within the region. Currently in the event of a crisis, sharing personnel and physical equipment among the Baltic States and neighboring region is difficult because there are extensive permissions required. Additionally, in the event of an emergency there would be limited personnel available. It is most likely that if one of the regional states were in a crisis situation, others would be as well, further limiting resources in the region. An example is the need to replace pole systems in the case of an emergency. Transmission connections among the Baltic States and with neighboring systems are critical to retaining the integrity of the combined power grid systems. The loss of such inter-system lines limits the operators' ability to respond effectively to other, compounding emergencies. The replacement of transmission towers can take weeks, or longer, depending on the circumstances. An emergency cooperation agreement outlining support for logistical supplies would allow for replacing pole systems faster. **Recommendation:** The system operator companies should consider signing official emergency cooperation agreements with their Baltic counterparts and those in Finland, Poland, and Sweden. These would be Inter-TSO agreements documenting requirements for solidarity and mutual support. There have been occasions of this sharing of resources on a Distribution System Operator (DSO) level. Agreements would have specific direction for mutual assistance between countries who share borders and/or infrastructure. These agreements would solidify the process of personnel and physical equipment being shared among the region in the event of a crisis.

Sense making and Information Fusion will be Targeted by Hybrid Threats. Syndicate members noted that indications during injects could be consistent and compatible with multiple types of failures: the presence of a hybrid-cyber attack, inaccurate reporting, or routine failures and faults in operational systems. Because of the Cyber Attack, confusion and prolonged inaction can result, particularly when combined with limited circulation of accurate and thorough reports. The confusion associated with hybrid attacks can lead to missed opportunities to avert attacks, delay external assistance, and limit operator action to mitigate effects. Additionally, the thresholds for hybrid reporting requirements are often subjective (i.e., they benefit from adjustment relative to potentially-related information in other domains). For example, the cumulative and/or sequential scope and threat of a sustained misinformation campaign leveraging deepfakes will change over time, just as the threshold for reporting equipment failures should lower as spares are consumed and/or system resilience is threatened. While Baltic States have well-established thresholds for invoking emergency procedures (e.g., loss of power for 24 hours to ¼ of a municipality or 20,000 residents in Lithuania - Regulations of Government of Lithuania 2006 march 9th – no. 241), thresholds and adjustments in response to hybrid and cyber threats such as network reconnaissance and exploitation, or incidents increasing the

possibility of civil unrest, are not standardized across the Baltic states. **Recommendation(s):** Establish and promulgate objective measures and associated responses for emerging threats to critical infrastructure, independent of a confirmed cyber or hybrid threat. While difficult, it is essential to establish frameworks (including thresholds) for aggregating, assessing, and responding to hybrid attacks. Robust, practiced (and automated, when possible) internal data reporting, integration, and enrichment can identify patterns and separate hybrid actions from routine failures and disinformation. While developing internal culture and processes, build inter-organizational and inter-national linkages to share, integrate, and analyze data. This reporting, analysis, and sensitivity can be thought of as a "hybrid security culture," similar to the best practice of establishing organizational cyber security cultures. To enable data collection, establish and promulgate objective reporting requirements for TSOs (Transmission System Operator) and their subordinates, and establish a central location for data fusion with well-defined lines of communication to political, military, and intelligence activities. For example: Establish tripwires for inter-state reporting of indicators that may be unusual in terms of duration, scope, and effects on redundancy. Indicators that require reporting may include malfunctions in non-redundant components affecting > 2% of power to the grid, malfunctions expected to persist longer than two weeks, or non-attributable failures in more than one designated critical component per TSO. Identification of effective indicators may require research and adaptation to specific industries in order to adapt to system-unique constraints (for instance, there are international dependencies in grid operations that do not exist to the same extent in medical infrastructure).

Whole of Government Coordination for Robust Communications. DSOs and TSOs must be able to maintain collaboration internationally (within Baltic States as well as with regional neighbors, not strictly following a hierarchical linkage) as well as internally (with the engineers in the field and at substations from different entities), even under direct and cascading effects of hybrid and cyber attacks. Processes were unclear for establishing secure communications and maintaining continuity of operations if all canonical communication systems were down (e.g., landlines, cell phones). National ministries did not have the same plan as TSOs and DSOs to rely on satellite phones for backup, and Syndicate representatives doubted there were sufficient numbers of satellite phones available to ministries. **Recommendation(s):** Establish and exercise primary, backup, and tertiary secure independent communications methods between and within key critical infrastructure elements in the Baltic States will ensure data flow even during a hybrid attack. Plans should (a) ensure access to means to communicate during emergencies and (b) consider sharing intelligence or military communication systems infrastructure (e.g., secure radio (UHF/VHF)) as required for continuity of operations under hybrid scenarios. In addition to establishing procedures for robust communications for DSOs and TSOs, training may be required on the operation of these communication systems and these contingency plans should be included in regional and national level exercises.

A number of key takeaways was identified by each of 4 syndicates and these are provided in the corresponding sections of the final exercise report [5].

4. CORE23-B TABLETOP EXERCISE

Coherent Resilience 2023 – Baltic (CORE 23-B) was a Tabletop Exercise on the energy system of the Baltic States with a focus on maritime critical energy infrastructure protection against hybrid threats. The Tabletop Exercise took place on 13-17 November 2023 in Riga, Latvia. The aim of the exercise was to support national authorities and key energy system stakeholders of the Baltic States and partnering nations with increasing the resiliency of their maritime energy installations and associated distribution networks in the Baltic Sea against hybrid threats. A spectrum of threats was introduced in the exercise scenario ranging from hybrid attacks and terrorism activities to conventional maritime operations. This exercise served as a collaborative venue to improve national contingency plans and procedures and develop NATO and the European Union capacity to support national authorities. CORE 23-B was a five-day regional, multilateral, interagency, and public-private sector event that was executed with an academic seminar, a three-day exercise, and a distinguished visitors' day that included after-action briefings. This report focuses largely on syndicate responses to the exercise scenario vignettes and injects to include capturing key takeaways and recommendations. The event brought together over 120 participants from 12 NATO and European Union countries or partner nations, who came from 45 different organizations representing maritime, energy supply and security stakeholders.

4.1. Scope and Objectives

The CORE 23-B TTX addressed critical energy infrastructure protection (CEIP) of the Baltic States and focused on protection of maritime and offshore energy installations in the Baltic Sea against hybrid attacks, terrorism activities and maritime operations. The main purpose of the exercise was to serve as a collaborative venue to improve national contingency plans and procedures, and develop NATO and the European Union capacity to support national authorities in protecting critical energy infrastructure while enhancing national and collective defence. The exercise design is based on the following underlying EU Regulations and Directives:

- Regulation (EU) 2019/941 on risk-preparedness in the electricity sector (Regulation 2019/941)
- Regulation (EU) 2017/1938 concerning measures to safeguard the security of gas supply (Regulation 2017/1938)
- Directive (EU) 2022/2557 on the resilience of critical entities (Directive 2022/2557)

The aim of the CORE 23-B TTX was to support the Baltic States and partnering nations national authorities and stakeholders in increasing of resiliency of maritime energy installations and transportation in the Baltic Sea against hybrid threats. CORE 23-B objectives were:

- Enhance resilience against hybrid threats on maritime energy infrastructure (including related installations in seaports) and Sea routes of transportation of the Baltic States
- Support the National authorities of the Baltic States, partnering nations and other stakeholders to improve its crisis management during hybrid attacks on maritime energy infrastructure (including related installations in seaports)
- Exercise cooperation and coordination of Strategic Communication (STRATCOM) among Baltic States energy sector parties in order to ensure timely and accurate dissemination of critical threat information and mitigation measures to all stakeholders in the region
- Identify and recommend best practices to mitigate gaps in existing and upcoming maritime legal frameworks, roles, process and procedures of nations, international organizations, the European Union, and/or NATO

The CORE 23-B TTX was prepared in a series of preparatory meetings. The initial planning conference took place at Military Academy of Lithuania (Vilnius, 14-15 February 2023), the main planning conference and vignettes/injects development workshop was hosted by AST, Latvian electricity system operator (Riga, 13-15 June 2023), and the final coordination conference took place at Estonian Ministry of Foreign Affairs (Tallinn, 19-20 September 2023). After the TTX, the post exercise discussion meeting took place in Vilnius, Lithuania (7-8 December, 2023).

Electricity supply in the Baltic States was simulated under disruption situation of each vignette [6]. This gave the participants insights on the consequences of the events to be discussed during the exercise. Participants were assigned to one of four different syndicate groups:

a) Critical Energy Infrastructure Protection (CEIP)
b) Crisis Response
c) Strategic Communication (STRATCOM)
d) Maritime Law.

4.2. Main findings

In the face of evolving hybrid threats to critical energy infrastructure, mechanisms for coordination, cooperation, and response between government/military/industry should also evolve across the EU. There are ambiguities and limitations in international law when it comes to classifying and responding to hybrid threats to energy systems. These ambiguities need to be addressed in part through exercises which examine specific likely threats. The broader syndicate team beyond their specific syndicates identifies the following key takeaway and recommendation of the exercise:

There is a need for increased awareness and understanding of critical energy infrastructure. There is currently no common understanding of what, exactly, constitutes critical energy infrastructure (CEI). The EU Directive defines CEI in generic way and attempts to standardize methods to identify and protect CEI are hindered by varying definitions of CEI and by individual approaches that may not be effective in a larger, collective context. While trends towards cross border energy distribution and interconnectedness are positive

and do increase the resilience and redundancy of our collective energy posture, they also bring risks if countries have varying definition of what energy infrastructure is. Furthermore, there is no common practice for instituting measures to protect CEI. This most certainly leads to weak points in the collective systems, which can be exploited by an adversary to achieve exponential effects across the whole system. **Recommendation:** Formal guidelines to learn how to determine which aspects of a country or region's energy infrastructure is critical is needed, probably followed by training and modelling. In addition to assessing the infrastructure and thinking about risks, the guidelines would also instruct participants regarding what steps are needed to protect CI, with the objective of increasing security, resilience, and redundancy.

The following takeaways are considered essential and deserve special attention by the decision makers:

Routine multi-national inspection of critical submarine pipeline/cables should be considered to baseline infrastructure security condition. The data collected during this assessment should be consolidated into a Common Operational Picture (COP) or Security Information and Event Management (SIEM) system to provide a high-level view of the infrastructure status/security, which can be shared. The established system would provide a common Point of Contact (POC) for Critical Energy Infrastructure. **Recommendation:** Form a Critical Energy Infrastructure Task Force or use already existing cooperation formats. This task force would have responsibility for identifying what infrastructure is deemed critical in each country and to the EU and Alliance. The use of modelling and simulations to determine this would be ideal. Once there is a common understanding of which infrastructure is deemed the most critical, then the task force could work to coordinate a means between government and private stakeholders to assess the security of this infrastructure and conduct regular multi-national inspections of that infrastructure. In addition to the increased security afforded by doing this, regular inspection intervals would also help narrow windows of malignant actions for the purpose of increased attribution when something does happen. In addition, the Task Force could play a role in conducting regional risk, threats, vulnerability assessments enabling countries to identify, evaluate and understand risks, threats and vulnerabilities of maritime critical infrastructure at regional level.

Current, legacy security systems and approaches are inadequate for the maritime threat we face today. The increasing use of unmanned aerial and maritime platforms by malign actors to avoid detection and inhibit attribution in the wake of an incident necessitates an ever-evolving approach to securing critical energy infrastructure. Our current systems are often not capable of detecting and/or responding to this type of threat. Furthermore, even when a threat of this nature is detected, national boundaries and parochial organizations hinder an effective response. **Recommendation:** Invest in advanced surveillance for improved drone detection, review and update legal frameworks, and conduct joint training for efficient collaboration. Implement a public awareness campaign to encourage vigilance and clarify legal boundaries. Strengthen cross-border information sharing, investigate drone infrastructure for attribution, and involve STRATCOM in managing public engagement. One possible way to coordinate with NATO and other allies is to participate in the NATO Critical Undersea Infrastructure Network. This could help to detect and deter any potential threats or challenges, and to enhance the security and the stability of the maritime sector. Another format would be to cooperate under implementation of the revised EU Maritime Security Strategy which also mentions EU-NATO cooperation as its key partnerships.

Enhancing EU energy strategic autonomy to manage energy delivery interruptions on the larger scale/regional crisis will mitigate impact of a crisis situation in terms of repair capacity for production and delivery systems. Short term resiliency in the energy sector is sustainable for "routine" incidents but is not sufficient for multiple and/or coordinated hybrid threats. Long waiting times in manufacturing and repair capability decreases crisis response. Lack of diversified local supply chains that are readily available and gaps in raw materials and technical skills to build replacements or restore existing infrastructure will decrease resiliency. Challenges to investments due to political issues and market forces result in this being a low priority. **Recommendation:** More precise deliberate long term planning is needed by first assessing critical asset components in the EU and their economic and societal importance and prioritizing their restoration/repair needs. Manufacturing, supply chain and repair capability gaps should be assessed and addressed to provide greater capability and capacity within the EU.

Coordinated communications deliver messages of unity to domestic audiences and deterrence to adversaries. Issuance of joint statements demonstrates prior coordination and alignment between allies.

Such action complicates an adversary's goal of maintaining strategic ambiguity to ultimately mitigate a unified response. Further, these communications provide assurance to domestic populations that their governments have credible plans and support from allies. **Recommendation:** Develop pre-planned messages to rapidly respond once preconditions are met. Operational mechanisms to develop and coordinate at EU level subsequent releases are crucial to ensure that follow-on actions and communications are coherent and reinforcing. Diplomatic messages, high-level visits from national-level EU and NATO leaders, media relations, and social media are tools that all can be leveraged to establish and maintain coordinated strategic communications.

Determining when an attack on critical infrastructure amounts to an armed attack on a State's sovereignty. Does a small physical attack, which has a large economic impact, amount to an armed attack? Does this depend on whether the attack occurs in territorial sea or EEZ? Attacks on privately owned CI are not clearly defined as attacks on a country. How can attacks be attributed to a state actor rather than a criminal group? Western legal frameworks are not well suited to dealing with hybrid warfare tactics. **Recommendation:** The Baltic region with the EU support should develop a unified response to attacks on CI and Hybrid warfare when CI is impacted. Poland has adopted or passed legislation that make it very clear that attacking underwater infrastructure is an attack on Poland. The Baltic countries should consider adopting similar legislation. Baltic countries should also consider joint legislation to spell out actions expected if cable/pipeline is attacked (e.g., board/confiscate nearby ships, etc.). Gaps in national laws should be closed by defining what constitutes an armed attack on underwater infrastructure, considering also possible unified EU approach.

A number of key takeaways was identified by each of 4 syndicates and these are provided in the corresponding sections of the final exercise report [7].

4. CONCLUSION

Looking backwards, we can clearly conclude that CORE19 TTX has stimulated and actually paved the way to signatures of inter-governmental agreements on natural gas solidarity among the Baltic States. While we could not identify such an obvious outcome from other two exercises, they clearly improved trans-national exchange on best practices, helped to identify gaps and missing procedures and proposed regional measures for further actions.

It is important to note that exercise reports – ideally – do not end exercises, for the region, nations, agencies and organizations that participated in those TTXs. They should each develop an Improvement Plan based on the relevant key takeaways identified. Each institution is to further analyse the key takeaways pertinent to them in order to identify the best means to facilitate improvements and develop the corresponding plan of action.

The participant's surveys conducted by NPS at the end of each exercise indicate the need and importance of such exercises. This need is in particular evident in this time of threats and attacks becoming more and more realistic.

We do believe that three exercises, all taking more than 6 months effort to organise and arrange, will contribute to the energy security and resilience improvements of the Baltic Sea region.

Acknowledgements

The authors acknowledge efforts of many contributors to the success of these exercises – mainly facilitators of syndicates, members of core planning teams, evaluation teams and participants themselves.

References

[1] FEMA. (2019). Discussion-based Exercises – Types, Goals, and Conduct. Federal Emergency Management Agency, Department of Homeland Security. URL: https://emilms.fema.gov/

[2] Vamanu, B., Martišauskas, L., Karagiannis, G., Masera, M., Krausmann, E., Kopustinskas, V., Development of indicator framework for resilience of critical energy infrastructure, European Commission, Ispra, 2021, JRC125802.

[3] Kopustinskas, V., Šikas, R., Walzer, L., Vamanu, B., Masera, M., Vainio, J. and Petkevičius, R., Tabletop exercise: Coherent Resilience 2019 (CORE 19) - Final report, EUR 29872 EN, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-11830-5, doi:10.2760/356320, JRC118083.

[4] Hybrid CoE Research Report. "Nuclear energy and the current security environment in the era of hybrid threats", ISBN 978-952-7282-2, 2019.

[5] Nave C., Kopustinskas V., Dirginčius E., Walzer L., Beniulytė G., Purvins A., Masera M., Nussbaum D., Norg V., Užkuraitis D. Tabletop exercise: Coherent Resilience 2021 Baltic (CORE21-B) - Final report, EUR 31020 EN, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-49466-9, doi: 10.2760/74397, JRC128730.

[6] Asensio I., Foretic H., Kopustinskas V., Modelling Power Disruption Scenarios in the Baltic Region using PyPSA, Proceedings of the ESREL 2024 conference: Advances in Reliability, Safety and Security, June 23-27, Cracow, 2024. (Accepted for publication).

[7] Dirginčius, E., Kopustinskas, V., Aukščionis, D., Lynn, C.B., Užkuraitis, D., Vlagsma, K., Nussbaum, D., Trakimavičius, L., Asensio Bermejo, I., Bazukaitė, P., Foretic, H. and Babilas, P., Tabletop exercise: Coherent Resilience Baltic 2023 (CORE 23-B), Publications Office of the European Union, Luxembourg, 2024, https://data.europa.eu/doi/10.2760/702667, JRC137990.