ISSN 1831-9424

Tabletop exercise: Coherent Resilience Baltic 2023 (CORE 23-B)

Final Report

Dirginčius, E., Kopustinskas, V., Aukščionis, D., Lynn, C.B., Užkuraitis, D., Vlagsma, K., Nussbaum, D., Trakimavičius, L., Asensio Bermejo, I., Bazukaitė, P., Foretic, H., Babilas, P.

2024

Joint Research Centre

EUR 31939 EN

Contact information
Name: Vytis Kopustinskas
Address: E. Fermi 2749, Ispra (VA), 21027, Italy
Email: vytis.kopustinskas@ec.europa.eu
Tel.:+39 0332 786257

EU Science Hub
https://joint-research-centre.ec.europa.eu

JRC137990

EUR 31939 EN

Print	ISBN 978-92-68-16150-0	ISSN 1018-5593	doi:10.2760/59946	KJ-NA-31-939-EN-C
PDF	ISBN 978-92-68-16151-7	ISSN 1831-9424	doi:10.2760/702667	KJ-NA-31-939-EN-N

Luxembourg: Publications Office of the European Union, 2024

How to cite this report: European Commission, Joint Research Centre, 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.

Contents

Abstract

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.

Acknowledgements

The authors acknowledge very active participation of many stakeholders – many of who had multiple roles – during preparatory meetings and during the main Tabletop Exercise event. In particular, the authors acknowledge the contribution of moderators who led syndicate discussions:

Syndicate 1 – Critical Energy Infrastructure Protection:
Ms. Chelsey SLACK (NATO HQ) and Mr. Natanael CARTAXO (DG ENER)

Syndicate 2 -Crisis Response:
Mr. Daniel O'CONNOR (US FEMA) and Ms. Isabel ASENSIO BERMEJO (JRC)

Syndicate 3 - STRATCOM:
Ms. Guna SNORE (NATO STRATCOM COE) and LTC Tomas BALKUS (Lithuanian Armed Forces)

Syndicate 4 – Maritime Law:
CAPT (N) Georgios GIANNOULIS (Hybrid COE) and CDR Philip von Eberhardt (NATO CSW COE)

The core planning team was leading development of the exercise scenario, vignettes and injects. Their efforts are greatly acknowledged:

The Core Planning Team Leader LTC Darius AUKŠČIONIS (NATO ENSEC COE) and the members: Dr. Vytis KOPUSTINSKAS (JRC), CAPT Evaldas DIRGINČIUS (NATO ENSEC COE), Mr. Lukas TRAKIMAVIČIUS (NATO ENSEC COE), Ms. Isabel ASENSIO BERMEJO (JRC), Mr. Hrvoje FORETIĆ (JRC), CDR H. Ceyhun TÜRE (NATO ENSEC COE)

The contribution and support to the core planning team of the following external experts was of utmost importance:

Mr. Charles LYNN (NPS), Ms. Paulė BAZIUKAITĖ (ESCD NATO HQ), Mr. Flemming Birck PEDERSEN (ENERGINET), Mr. Per Olav FOSS (Equinor), CAPT (N) Georgios GIANNOULIS (Hybrid COE), LT (N) Alexandru-Cristian HUDIȘTEANU (NATO MARSEC COE)

The authors greatly acknowledge the exercise lecturers for their knowledge sharing and interactions:

Mr. Isto MATILLA (Laurea University, Finland), Mr. Per Olav FOSS (Equinor AS, Norway), Mr. Aykut KERTMEN (Meteksan Savunma Sanayi A. Ş., Turkey)

The authors acknowledge excellent contribution of the TTX Evaluation group in collecting information for this report: CAPT Matthew Ahlers (USN Reserves), CDR Chad Brahler (USN Reserves), LCDR David Carroll (USN Reserves), Col Michael Davis (USA, ret.; NPS), CAPT Dewey Devins (USN Reserves), CDR Regis Dowd (USN Reserves), Dr. Victor "Bob" Garza (NPS), LtCol Charles Lynn (USMC, ret; NPS), Dr. Michael Malley (NPS), LCDR Ethan Mansel (USN Reserves), Dr. Daniel Nussbaum (NPS), LT Michael Parker (USN; NPS), CDR Shelia Sklerov (USN Reserves), CAPT Micheal Sullivan (USCG, ret.; US DHS), and LCDR Jefferey Withington (USN Reserves).

Authors:

Evaldas Dirginčius, Vytis Kopustinskas, Darius Aukščionis, Charles B. Lynn, Darius Užkuraitis, Kristine Vlagsma, Daniel Nussbaum, Lukas Trakimavičius, Isabel Asensio Bermejo, Paulė Bazukaitė, Hrvoje Foretić, Paulius Babilas.

1 Introduction

Coherent Resilience (CORE) is a series of national and regional level tabletop exercises (TTX) aimed at enhancing resilience of energy systems in an era of hybrid threats. CORE TTXs have been conducted as national and regional programs in the Baltic States as well as in Ukraine, Georgia, Moldova and other countries. Coherent Resilience 2023 - Baltic (CORE 23-B) was the third Baltic region TTX jointly organized by the European Commission's Joint Research Centre (JRC) and the NATO Energy Security Centre of Excellence (ENSEC COE). The CORE23-B follows excellent feedback and experience gained during execution of CORE-21B (Nave et al., 2021) and CORE-19 (Kopustinskas et al., 2019) tabletop exercises.

This report constitutes the final report of the CORE23-B Tabletop exercise, jointly co-organized by the NATO Energy Security Centre of Excellence and the European Commission's Joint Research Centre. The exercise was evaluated by the Naval Postgraduate School (NPS), which also drafted the final report. 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 TTX took place on 13-17 November 2023 in Riga, Latvia. The event brought together over 120 participants from 12 NATO and European Union countries or partner nations. All 8 EU Member States around the Baltic Sea were present and Norway as a member of the European Economic Area. The participants came from 45 different organizations representing maritime, energy supply and security stakeholders (**Figure 1**). **Table 1** in Annex 1 captures the list of participating organizations.

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).

Figure 1. CORE23-B Participants «Family Photo»

Source: NATO ENSEC COE, 2023.

2 CORE 23-B Tabletop Exercise design

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)

2.1 Purpose, Aim, Objectives

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

2.2 Concept for the Event

CORE 23-B was opened by welcome messages of COL Darius Užkuraitis, Director of NATO ENSEC COE (**Figure 2**, right) and Dr. Habil. Piotr Szymański, Director of Directorate C – Energy, Mobility and Climate of the JRC (**Figure 2**, left).

The TTX was divided into three phases that included an academic seminar, the tabletop exercise, and the distinguished visitors' day/after action session. The TTX lecturers and the audience are captured in **Figure 3**.

Phase One, the academic seminar consisted of a series of expert presentations to better prepare participants for the TTX. Lectures included the following topics:

1. Maritime Security Strategy with focus on the protection of Undersea Energy Infrastructure by Capt. (N) (ret.). Isto MATILLA, Laurea University, Finland;
2. Main learnings after Equinor's pipeline security inspections by Mr. Per Olav FOSS, Equinor;
3. Modern technologies for maritime security by LCDR (ret.) Aykut KERTMEN, METEKSAN;

Figure 2. CORE23-B welcoming remarks

Source: JRC, 2023.

After the academic lectures, TTX details were presented to the participants, serving as a transition to second phase of the exercise. The TTX Scenario and Vignettes were presented by the core planning team leader - Lt Col Darius Aukščionis (NATO ENSEC COE). It followed by the JRC slot of presentations. The first part was done by Kristine Vlagsma, Head of Energy Security, Distribution and Markets Unit, who presented JRC in general and the unit activities. The second part was done by Isabel Asensio, who presented results of modelling performed at the JRC by PyPSA (Python for Power System Analysis) modelling tool (Asensio et al., 2024). PyPSA is an open source tool (Brown, 2018 & Hörsch, 2018) that recently gets a widespread use in academic environment and by system operators.

Electricity supply in the Baltic States was simulated under disruption situation of each vignette. This gave the participants insights on the consequences of the events to be discussed during the exercise.

Phase Two of CORE 23-B was the execution of the TTX, the main event of the five-day program. Participants were assigned to one of four different syndicate groups:

1. Critical Energy Infrastructure Protection (CEIP)
2. Crisis Response
3. Strategic Communication (STRATCOM)
4. Maritime Law.

In addition to the participants, each syndicate had two Co-Facilitators to lead discussions and a small cell of evaluators. NPS has conducted a survey of the participants that is presented in Annex 2.

Phase Three of CORE 23-B consisted of the TTX After Action (Hot Wash) and coincided with the Distinguished Visitors' Day (DVD). This phase allowed each Syndicate to have presenters brief their syndicate assessment and response to a selected inject and highlight overall syndicate outcomes regarding identified areas for improvement and best practices. The distinguished visitors consisted of an impressive group of senior officials, diplomats, and industry representatives. The DVD participants were addressed by Mr. Rolands Heniņš, Policy Director at Ministry of Defence of Latvia, Ms. Salla Saastamoinen, Deputy Director General of the JRC, (**Figure 4**), Ms. Chelsey Slack representing NATO Headquarters and Mr. Ignas Jonynas, Deputy Head of Unit at Secretariat-General of the European Commission, (**Figure 5**). The DVD continued by presentations of all syndicates on the main findings and takeaways and presentation on the exercise evaluation process by C. Lynn, NPS evaluation team leader. The DVD was closed by NPS Energy Department chair Dr. D. Nussbaum and Director of NATO ENSEC COE COL. D. Užkuraitis.

Figure 3. TTX presentations and audience

Source: JRC, 2023.

Figure 4. Deputy Director General of the JRC, Ms. Salla Saastamoinen opens Distinguished Visitors Day.

Source: JRC, 2023.

Figure 5. Deputy Head of Unit at Secretariat-General, European Commission, Mr. Ignas Jonynas welcomes participants at Distinguished Visitors Day.

Source: JRC, 2023.

2.3 Exercise Scenario, Vignettes and Injects

The exercise scenario sets a background situation and environment of the exercise. Typically the environment for the CORE exercises is very hostile and full of geopolitical challenges.

What is a vignette? Typically, vignettes provide a high-level overview describing a significant crisis situation used to illustrate or identify a particular issue. These overviews are provided in the context of the overarching scenario. A vignette is a brief description, account or episode which evokes strong images, memories, or feelings. A vignette-based Tabletop Exercise is an exercise that uses the vignette details as the exercise setting and situation. In other words, it is a situation with relatively large consequences that demands reaction from the participants.

What is an inject? If a vignette is a specific development within the overarching scenario, then an inject is a specific event within a vignette. An inject is a short event story used to bring an incident to the players' attention for whom it was created (and from whom a reaction is expected). In other words, it is an incident with relatively small and local consequences that demands reaction from a selected part of the participants. Different injects can be used under the same vignette for different discussion groups (also called syndicates).

CORE23-B TTX training audience discussed three vignettes that unfold over the course of three, consecutive months. In total 18 injects were prepared with the three vignettes. The exercise scenario, vignette and inject details were provided to the exercise participants.

2.4 Final exercise report

This report focuses largely on the syndicate responses to the scenario vignettes and injects, and it captures the key takeaways - areas of improvement, best practices, and recommendations. The next section begins an overview of the exercise scenario, vignettes, and injects. Readers will note that not every inject has a response, for either some injects did not relate to the syndicate or the syndicate did not have time to respond to each inject. At the end of each syndicate section, there is a sub-section that provides the syndicate key takeaways. The concluding section of the report captures the broader key takeaways that are relevant beyond one syndicate.

Readers will note that the exercise was based on a fictional scenario that closely resembles regional realities, Accordingly, syndicate responses are completed in line with the scenario. However, where applicable, the key takeaways are captured using actual country names etc.

Exercise evaluators captured and provided draft syndicate responses and key takeaways that were reviewed, refined, and expanded upon during a post exercise discussion in Vilnius, Lithuania on 7-8 December 2023, where several facilitators, participants, and evaluators gathered to develop much of the final content of this report – it was a team effort.

3 Syndicate Takeaways

This section provides major takeaways developed in each of the four syndicates. The participants have raised many more ideas and comments, but not each single comment or idea could have been developed into a major takeaway of each syndicate. This just indicates that the exercise was a kind of idea generator that triggered a lot of thinking and reactions from the participants, ideally brought back to their organisations after the event.

3.1 Syndicate 1: Critical Energy Infrastructure Protection

The syndicate work view is shown in **Figure 6**.

Figure 6. Critical Energy Infrastructure Protection Syndicate during discussions

Source: NATO ENSEC COE, 2023.

Key Takeaways and Recommendations

A more proactive approach is needed to identify roles, responsibilities, and authorities related to crisis response. Some countries have cooperation agreements in place, which define roles, responsibilities and authorities between government agencies and utility providers and operators. Countries that are still developing their approach to crisis management should consider these models. Particularly when it comes to the linkages between the public and private sectors. Key questions to answer are: What requirements do operators need for protection?; What are the main risks to critical infrastructure protection?; Are there secure communication channels to affect coordination in an emergency?; Who are the primary points of contact in each sector who need to be working together ahead of time to ensure effective and efficient crisis action response? **Recommendation**: Develop detailed, holistic crisis response plans that identify those stakeholders who play a part in crisis response well ahead of an actual crisis. Exercise those plans regularly to ensure that everyone understands both their individual responsibilities and the collective responsibility when a crisis occurs.

Encouraging robust collaboration for maritime/undersea pipeline/cable inspections, including the sharing of best practices, and developing protocols for information exchange and advisories across public and private sectors, is crucial for enhancing collective preparedness. Emphasis should be placed on integrating safety and security mind-sets and maintaining a balance between technical integrity surveillance and security measures. Standardized, coordinated inspections, coupled with clearly defined reporting responsibilities among security and industrial entities, should be prioritised. Additionally, it is essential to address geopolitical considerations, particularly during military exercises, to prevent interference and ensure the safety and security of critical infrastructure. **Recommendation**: Establish formal and informal arrangements between infrastructure operators and governments during peacetime, exploring all available EU wide cooperation formats, including Electricity Coordination Group, Gas Coordination Group or Critical Entity Group or other formats organised by the EC services. This should be complemented by fostering regular discussions to share technical knowledge and sector-specific threat assessments while harmonizing inspection frequencies on an international scale. Encouraging robust collaboration for maritime pipeline/cable inspections, including the sharing of best practices, and developing protocols for information exchange and warnings/advisories across sectors and governments, is crucial for enhancing collective preparedness.

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 (EUMSS) which also mentions EU-NATO cooperation as its key partnerships.

Collaborative training and effective rehearsals are key to skilfully managing critical infrastructure-related crisis events in the Maritime environment. The exercise posed several scenarios where events threatened both the security of critical energy infrastructure and the supply of energy associated with that infrastructure. The adverse effects of these events were exacerbated by the vagaries of international and maritime law. In each of these fictional but potentially likely events, the key to an effective response was working across traditional boundaries, both organizational and national, to ensure that each of the agencies that might have a role in the response are coordinating ahead of time. Doing so helps to prevent a situation where the agencies involved are having to build communications channels and relationships during an actual crisis. **Recommendation**: Conduct regular collaborative training, both internal to countries and between countries, where the agencies that would have to respond to a maritime security threat to critical infrastructure are compelled to cooperate to respond to the threat situation. Identify key stakeholders in both the government and private sector, then develop an understanding, through practical application in the form of exercises and rehearsals, of what role each of these organizations would play and what their shortfalls are. Seek to mitigate those shortfalls by taking a unified approach in which organizations mutually support each other.

Diversification of Energy Sources and Critical Energy Infrastructure are pre-crisis protection measures. Too often, there are single points of failure in our energy supply chains. The impacts of a single pipeline or terminal being degraded or destroyed can have enormous effects across multiple regions. It is prudent to think that our adversaries realize this factor and intend to take advantage of it to achieve their ends. Diversifying energy sources, supply routes and the related energy infrastructure that is required for transportation and distribution is a wise crisis mitigation measure. **Recommendation**: Explore alternative ways to secure the energy supply, such as diversifying the sources, increasing the storage capacity, or using other modes of transportation such as rail or pipeline. This could involve investing in renewable energy, building strategic reserves, or developing infrastructure and agreements with other partners. The principal barriers to building redundancy into these systems seem to be a desire for optimization and a desire to cut costs. Further analysis will show that the costs of not having redundancy built into the system when it is attacked are much higher, across a range of effects, than having allocated the resources in the beginning.

3.2 Syndicate 2: Crisis Response

The syndicate work view is shown in **Figure 7**.

Figure 7. Crisis Response Syndicate during discussions

Source: NATO ENSEC COE, 2023.

Key Takeaways and Recommendations

Baltic Sea regional collaboration should be developed in advance of hybrid and/or prolonged energy crisis situations to maintain trust and solidarity between countries. Intergovernmental cooperation in devising a coordinated response is critical to crisis response. National forums exist internally within all countries. Energy providers share information and status; Contributing to and access of common operating picture leads to better understanding and cooperation. Establishing and maintaining regional forums to resolve issues are needed. Sharing information between Member States and nations through bilateral and multilateral agreements define areas of collaboration in advance. **Recommendation**: Agreements need to be in place for governments to sustain solidarity agreements during emergencies or crisis. Currently, many solidarity agreements has been already signed in the gas sector under Regulation EU2017/1938 and discussions are taking at the ECG for the electricity sector solidarity. Maintaining relevant contacts across region/across sectors including industry, private, governmental, military, and cyber will facilitate cooperation. A crisis will be interlinked across multiple sectors; forums to provide qualified technical advice to governments is needed.

Enhancing energy resilience with regards to critical infrastructure and in the population will assist mitigating crises across government and private sector entities and could serve as a deterrence to aggressors. Resiliency gaps in regional energy provision during a crisis can lead to shortages. Markets will drive investments to enhance resiliency – to a certain point. There are limits to what markets will support. Governments will conduct gap analyses and step in for long term planning agreements and manage financing to develop resources and educating the public in preparing for and managing energy delivery interruptions. **Recommendation**: Ensuring similar and coordinated approaches throughout the region by sharing best practices will provide enhanced resilience and will transcend national plans. Understanding capacity and capability gaps in advance is a critical element of crisis response. Explore and expand possibilities to close identified gaps through investing in and developing sharing mechanisms in energy and other resources (such as spare parts, human resources, technical capabilities, tools, transportation, icebreaking capabilities, etc.) within the Baltic Sea region and increase capacity to conduct repairs within EU.

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.

Developing and maintaining secure maritime routes and capabilities, as well as monitoring offshore assets are keys to consistent energy delivery. This includes keeping shipping lanes open as well as protecting critical infrastructure. In addition, assuring adequate regional repair capacities pose challenges. Harsh winter conditions when navigation is needed under freezing temperatures in ice covered waters, or under spray icing presents unique challenges to the region as well. Government and industry cooperation is required to sustain needs for both funding, subsidizing and building capabilities. **Recommendation**: Maritime domain awareness should be improved and readily shared to enhance solidarity and facilitate resource allocation decisions. Improving regional cooperation and maritime resource sharing will strengthen capabilities and serve as a deterrent. The ability to conduct repair operations in a challenging environment is influenced by market forces and the current and projected needs should be evaluated at regional level.

3.3 Syndicate 3: Strategic Communication

The syndicate work view is shown in **Figure 8**.

Figure 8. STRATCOM Syndicate during discussions

Source: JRC, 2023.

Key Takeaways and Recommendations

A mechanism is needed to coordinate governmental and cross-governmental strategic communications. In the event of a routine occurrence or a crisis, a mechanism is needed to coordinate a governmental response and/or messaging (e.g. an investigation). The key role of such exchange would be to collate and cascade information across borders to and from various government ministries and organizations, including the EU and NATO. **Recommendation:** Establish an exchange mechanism in a form of joint working group or a task force, comprising members from relevant institutions and authorities, energy companies and TSOs. Such an entity could also mitigate adversary STRATCOM messaging that seeks to undermine solidarity among the Member States.

Member States should consider developing a process and/or body for the investigation of maritime incidents possibly supported by EU bodies. The US National Transportation Safety Board (NTSB) might serve as an example. **Recommendation:** Develop EU or international maritime investigation protocols. Additionally, such an investigative organization might be able to establish protocols for sharing and vetting cyber security threats related to such maritime damages.

Do not dismiss adversary propaganda. NATO STRATCOM professionals and policymakers should avoid national biases against adversary media 'facts'. While many NATO nations question the validity and value of adversary STRATCOM/propaganda, STRATCOM professionals must understand minority audiences within their borders, as well as the role of propaganda in wider international domains (e.g.

China, the Global South, etc.), and within the adversary nation itself. **Recommendation**: NATO and Baltic Sea allies should consider combatting adversary strategic messaging within adversary borders and within non-aligned nations.

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.

Communication is vital during energy disruptions. During energy crises, brownouts or load shedding remain a vital tool to maintain the function of the energy grid. Removing uncertainty of when brownouts will occur allows citizens to prepare and mitigate negative impacts. **Recommendation**: During pre-crisis phases, national governments should develop national communications plans and should encourage homes to maintain backup equipment, like radios or batteries. During energy shortages, member States should leverage the existence of national emergency communications channels and facilities. TSOs should provide and communicate load shedding schedules and instructions to the public on minimizing energy usage.

3.4 Syndicate 4: Maritime Law

The syndicate work view is shown in **Figure 9**.

Figure 9. Maritime Law Syndicate during discussions

Source: JRC, 2023.

Key Takeaways and Recommendations

Authorization to anchor in the vicinity of critical energy infrastructure. According to UNLCOS, maritime vessels have few limitations where to anchor and there is no legal basis for asking a ship to move. UNCLOS allows States to establish a safety zone up to 500 meters around offshore installations, which may be considered as critical infrastructure (CI), but at the same time UNCLOS does not expressly recognize enforcement jurisdiction to the State which erected the safety zone. However, such a form of jurisdiction could be interpreted from UNCLOS if the ship threatens the sovereign rights of the coastal State in the EEZ (i.e. exploit resources and establish safety zones). To tow it away against the will of the ship's master would require national legislation, which does not currently exist. Jurisdiction to take actions against the ship are not clear. **Recommendation**: Evaluate national laws to discern jurisdiction to have a maritime vessel removed from the safety zone around a CI and ensure it is clear as to who has the jurisdiction (i.e. the CI owner or the coastal state authority). Review national laws to ensure appropriate laws/legal framework are in place for a State to forcefully move a ship out of safety zones or to a safer area; delineate who is responsible for moving the ship. Some thought also needs to be given to defining enforcement jurisdictions and ensuring that safety zones are appropriately defined and jurisdiction is captured in some legal framework.

Rights of coastal states in their exclusive economic zone (EEZ). In situations where illegal activity, including potential terrorism, is discovered within EEZ, international law governing cables and pipelines on the seabed is vague. This is further compounded when non-attributable actions occur while another country is conducting naval exercises or other activity in those regions. Because of this ambiguity, a coastal state's jurisdiction over events that transpire on the high seas (i.e.; outside of their territorial waters) is not clearly defined. **Recommendation**: The Baltic Sea countries should consider establishing a mutual agreement to define maximum length of military exercises in the Baltic Sea to ensure freedom of navigation is not disrupted. They also should consider establishing policies and procedures that enable cable and pipeline owners to inspect their property in EEZ and territorial sea. Multi-lateral agreements such as these can, in many cases, mitigate the areas where the law of the sea has not evolved fast enough to be effective.

National responsibility for unexploded ordnance (UXO) in territorial sea. Jurisdiction for UXO in a territorial sea rests with the coastal state whose territory the UXO is discovered in. Typically, a country's environment ministry would be responsible for clean-up. In these cases, legal authorities would begin an investigation immediately. In practice, there are often gaps between the various agencies who would each play a role in a situation like this. A common approach to an effective response can be hindered by varying understandings of the roles, responsibilities, and authorities of key stakeholders in the response. **Recommendation**: Agencies who would likely play a role in the response need to conduct collective planning and rehearsals before there is an actual event. Developing a national or regional response plan and regularly testing it are highly recommended. In the spectrum of the response, from initial first responders all the way to post-incident actions such as clean up and strategic messaging, there needs to be a common approach to avoid making a bad situation worse by poor procedures.

UAV Passage. From a legal perspective, regulation of drones in in its infancy. Further does a UAV have the right to innocent passage or is all passages by a UAV to be considered not innocent? Inside national airspace, the state clearly has jurisdiction and most states impose limits on civilian drones. However, these limits are not consistent across countries in the same region, not the same in the EEZ. **Recommendation**: Create a common understanding and legal framework related to UAVs within countries and within the region. In particular, how close and how high when near or above CI. Ensure that national laws clearly delineate action and who has authority if an unauthorized drone is detected in national air space.

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.

4 Concluding Exercise Key Takeaways and Recommendations

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 (CER, 2022) define 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.

5 Concluding Remarks

It is important to note that this report – ideally – does not end CORE23-B, for the region, nations, agencies and organizations that participated in the TTX. 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 exercise organisers will reach out to CORE participants at various points in the future to survey participants on any improvements that were implemented based on what was learned from CORE23-B.

The participant's survey conducted by NPS at the end of the exercise indicates 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 this exercise being more than 6 months effort to organise and arrange, will contribute to the security improvements of the Baltic Sea region.

The key achievements of the CORE23-B Tabletop exercise are condensed into key takeaways of each syndicate (**see Chapter 3**) and the exercise key takeaways (**see Chapter 4**).

References

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).

Brown T., Hörsch J. and Schlachtberger D., 'PyPSA: Python for Power System Analysis', *Journal of Open Research Software*, Vol. 6, No. 1, 2018, https://doi.org/10.5334/jors.188.

Directive 2022/2557, 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. *OJ L 333, 27.12.2022, p. 164–198*.

Hörsch J., Hofmann F., Schlachtberger D. and Brown T., 'PyPSA-Eur: An Open Optimisation Model of the European Transmission System', *Energy Strategy Reviews*, Vol. 22, 2018, pp. 207–215, https://doi.org/10.1016/j.esr.2018.08.012.

Regulation 2017/1938, Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010. *OJ L 280, 28.10.2017, p. 1–56.*

Regulation 2019/941,•Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC. *OJ L 158, 14.6.2019, p. 1–21.*

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.

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.

List of abbreviations and definitions

Abbreviations	Definitions
CORE	Coherent Resilience
CI	Critical Infrastructure
CEIP	Critical Energy Infrastructure Protection
COP	Common Operational Picture
CSW COE	Centre of Excellence for Operations in Confined and Shallow Waters
DVD	Distinguished Visitor Day
EEZ	Exclusive Economic Zone
ENSEC COE	Energy Security Centre of Excellence
EC	European Commission
FEMA	Federal Emergency Management Agency
HYBRID COE	European Centre of Excellence for Countering Hybrid Threats
JRC	Joint Research Centre
MSA	Maritime Situational Awareness
MARSEC COE	Maritime Security Centre of Excellence
NPS	Naval Postgraduate School
NTSB	National Transportation Safety Board
PyPSA	Python Power System Analysis
SIEM	Security Information and Event Management
STRATCOM COE	Strategic Communications Centre of Execellence
UAV	Unmanned Aerial Vehicle
UNCLOS	United Nations Convention on the Law of the Sea
UXO	Unexploded Ordnance
TSO	Transmission System Operator
TTX	Tabletop Exercise

List of figures

List of tables

Annexes

Annex 1. Participating Organizations

Table 1. List of participating organizations.

Participating Organizations	
1.	Ministry of Climate of Estonia
2.	Ministry of Energy of the Republic of Lithuania
3.	Ministry of Foreign Affairs of the Republic of Latvia
4.	Ministry of Foreign Affairs of the Republic of Estonia
5.	Ministry of National Defense of the Republic of Lithuania
6.	Ministry of National Defense of the Republic of Latvia
7.	Ministry of National Defense of the Republic of Estonia
8.	Danish Energy Agency
9.	Ministry of National Defense of Finland
10.	The European Centre of Excellence for Countering Hybrid Threats
11.	AB Litgrid (Lithuania)
12.	AS Elering (Estonia)
13.	Augstsprieguma Tīkls AS (AST) (Latvia)
14.	AS Conexus Baltic Grid (Latvia)
15.	Klaipėda Seaport (Lithuania)
16.	AS Klaipėdos nafta (Lithuania)
17.	AB Orlen Lietuva (Lithuania)
18.	Fingrid OYJ (Finland)
19.	Svenska Kraftnät (Sweden)
20.	UK's Department for Energy Security and Net Zero
21.	Equinor ASA (Norway)
22.	Government Office of Estonia
23.	Ministry of Interior Affairs of Republic of Lithuania
24.	Public Security Service of Republic of Lithuania
25.	State Border Guard Service of Republic of Lithuania
26.	Norwegian Communication Authority (NKOM)
27.	Ministry for Climate and Energy of the Republic of Latvia
28.	Ministry of Foreign Affairs of the Republic of Lithuania
29.	Ministry of Transport and Communication of Finland
30.	National Crisis Management Centre
31.	Finish Defence Forces
32.	National Emergency Supply Agency of Finland
33.	Ventspils seaport (Latvia)
34.	Energinet (Denmark)
35.	Equinor ASA (Norway)
36.	National Crisis Management Centre, (Lithuania)
37.	Polskie Sieci Elektroenergetyczne SA (PSE) (Poland)

38.	European Commission, JRC
39.	NATO HQ Emerging Security Challenges Division
40.	NATO Maritime Security Centre of Excellence
41.	Embassy of Japan in Lithuania
42.	Permanent representation of Spain to NATO
43.	NATO Crisis Management and Disaster Response Centre of Excellence
44.	Ministry of Defense Japan
45.	Naval Postgraduate School

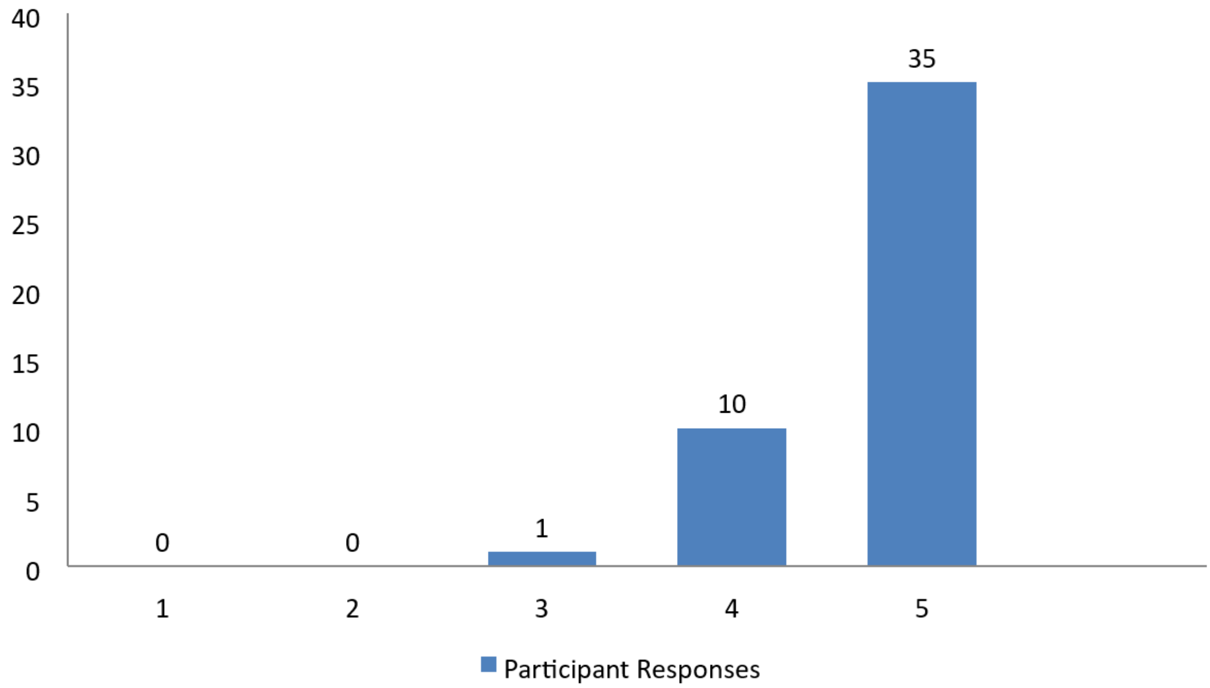
Source: ENSECCOE, 2023.

Annex 2. Results of Participant Exercise Evaluation Survey

This annex presents results of a two part survey that was conducted by NPS during the execution of the exercise. All participants were invited to participate, and around half of the participants responded. Below you see all the answers provided to each question asked.

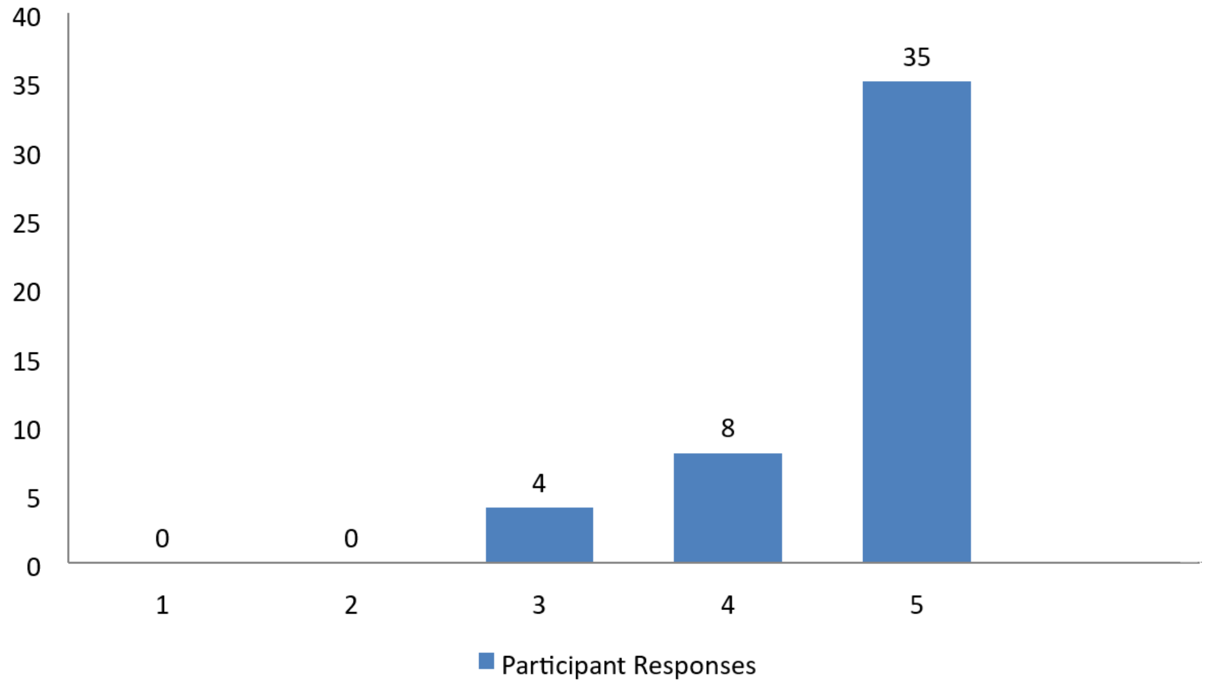
Quantitative Response Part I – focus on personal participation

1. Having regional nations participate in this TTX highly benefitted the event.



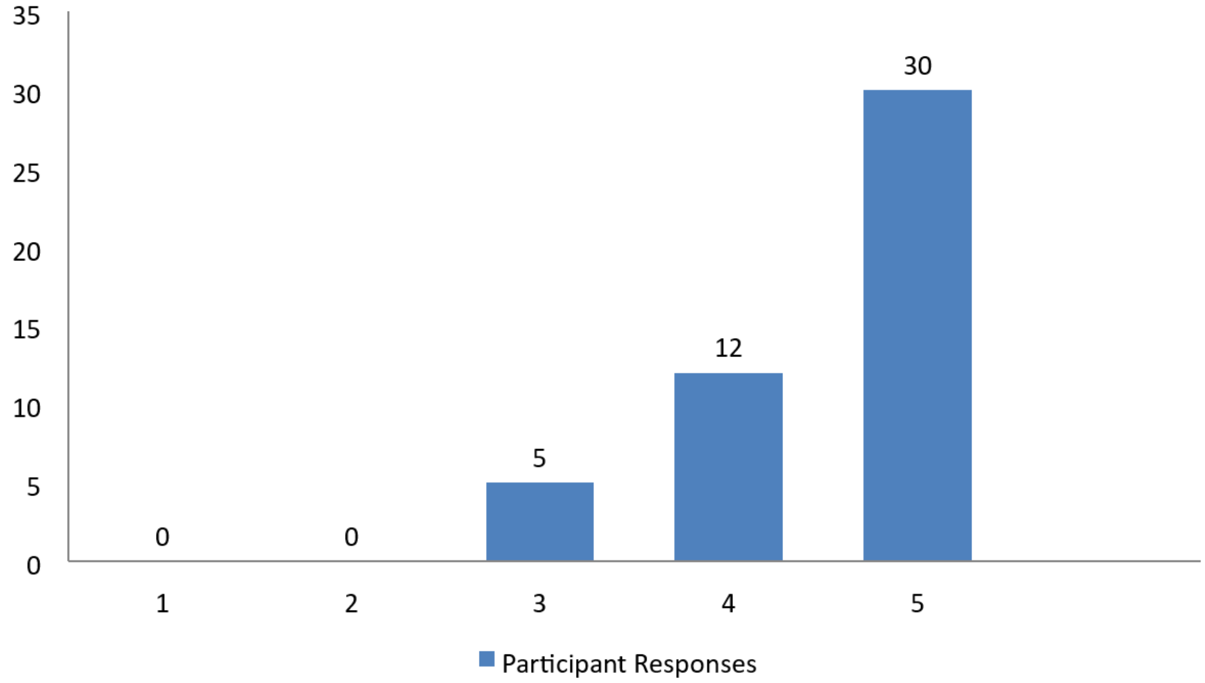
Source: NPS, 2023.

2. Having a mix of inter-agency representatives highly benefitted the event.



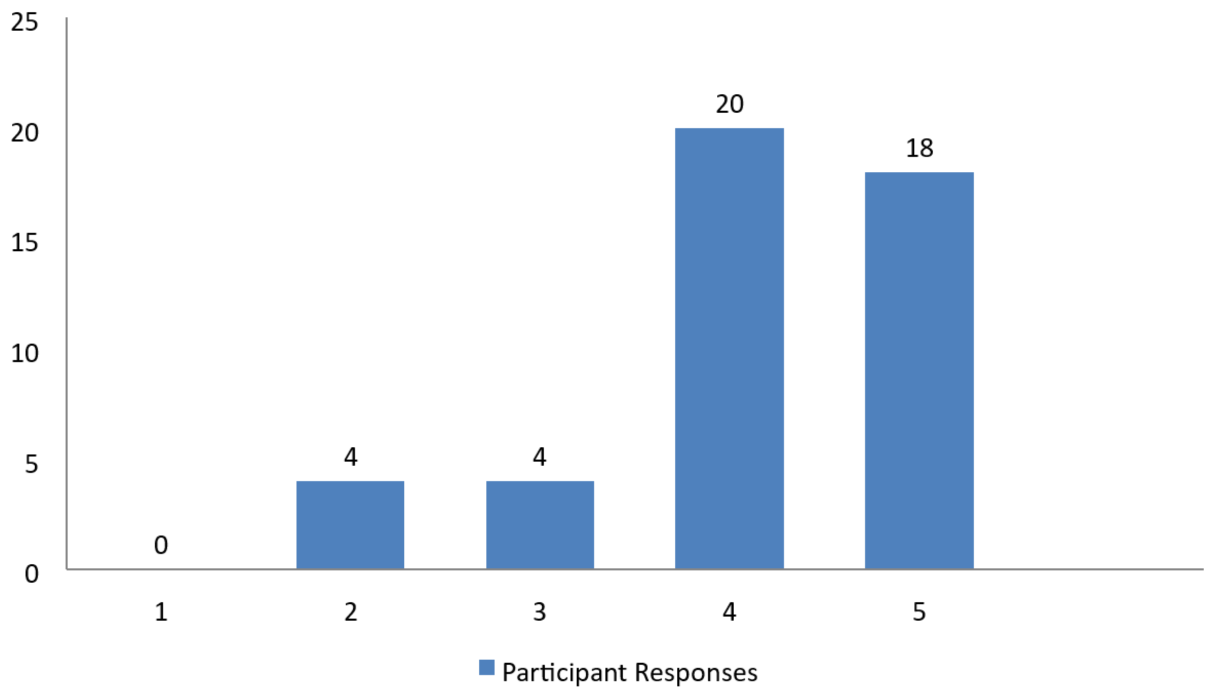
Source: NPS, 2023.

3. There should be more regional or national exercises (TTX, National Command Post, etc.) in the future.



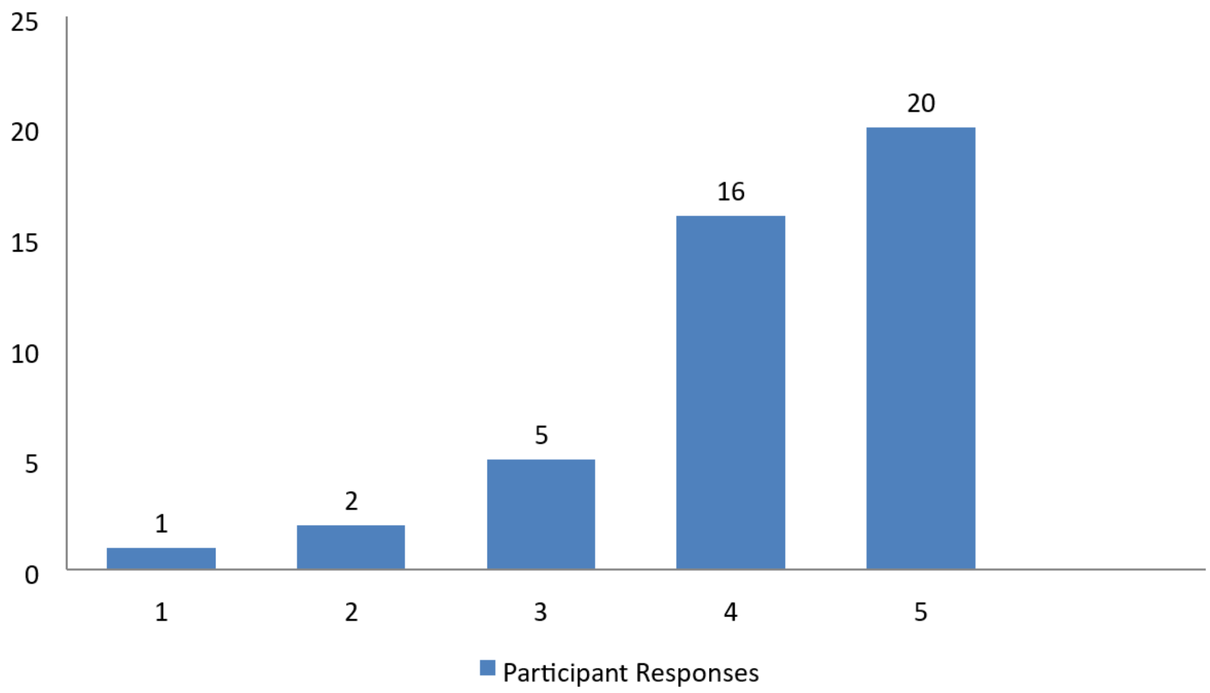
Source: NPS, 2023.

4. My participation in CORE TTX was very beneficial for my current job duties.



Source: NPS, 2023.

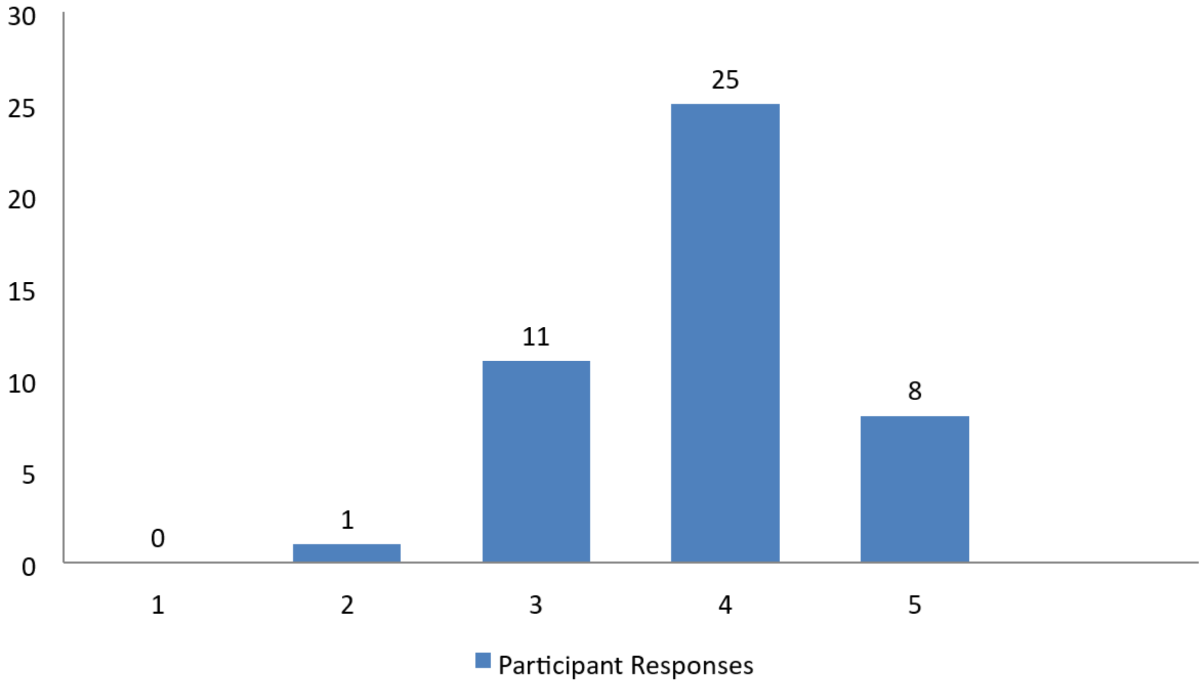
5. Participation in CORE TTX would be beneficial to my colleagues were they able to attend.



Source: NPS, 2023.

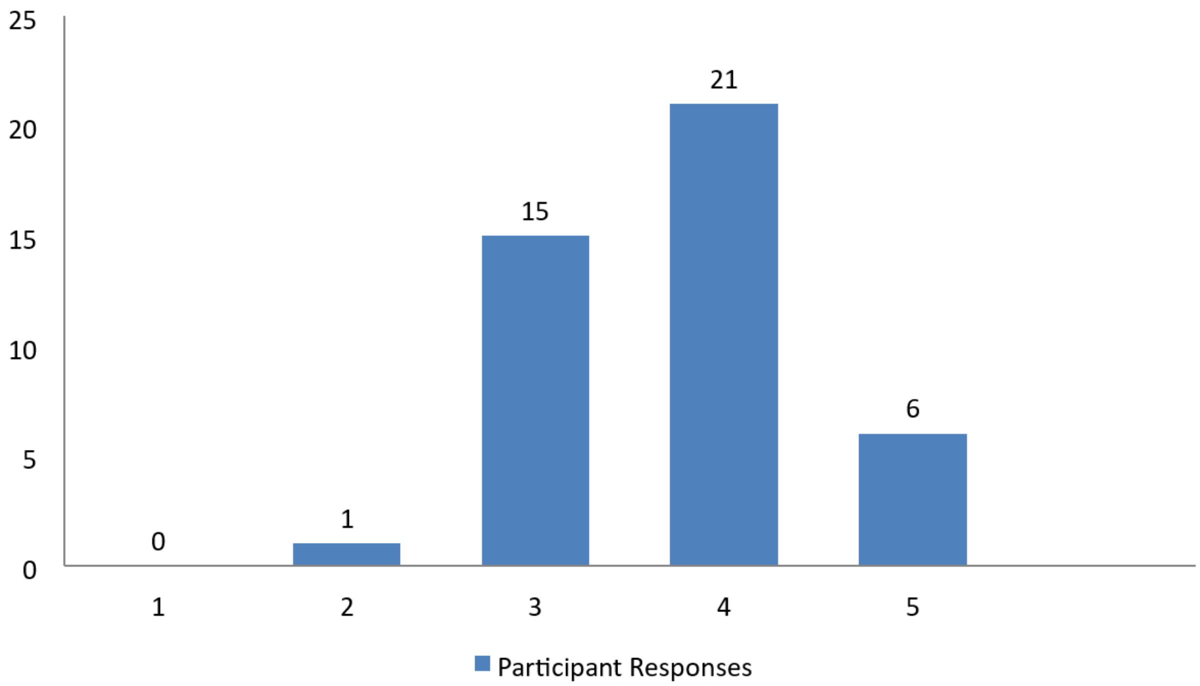
Quantitative Response Part 2 – focus on institutional participation

1. How would you rate the strength of your agency with regard to collaborating with other agencies?



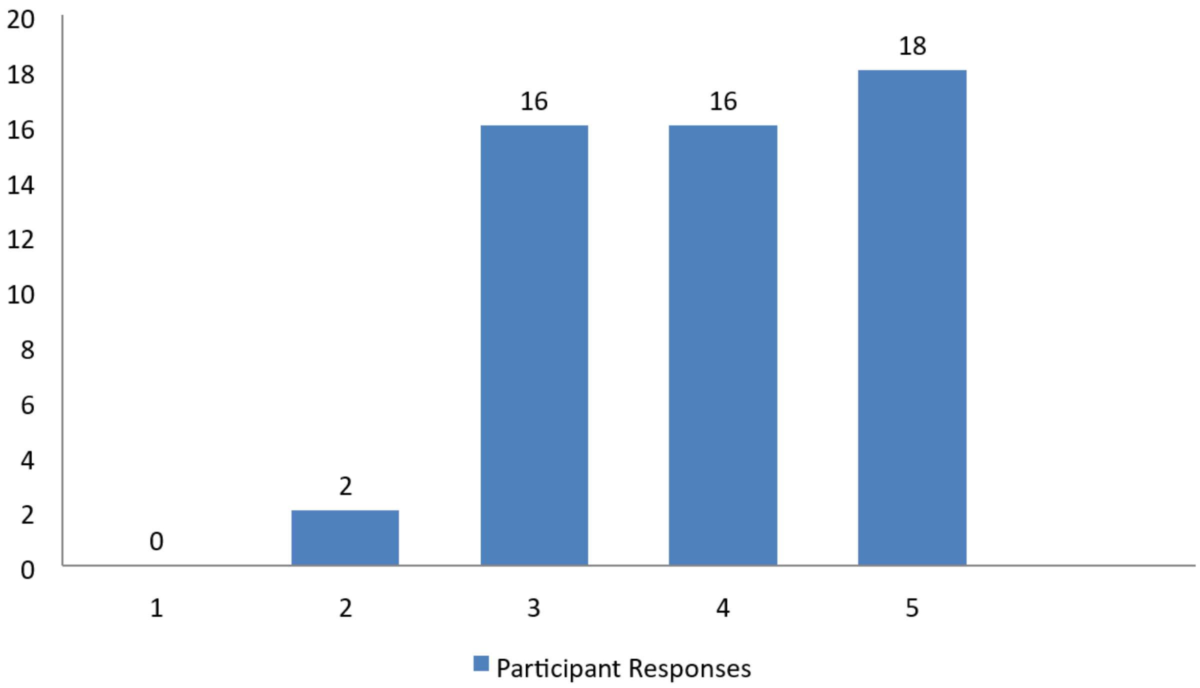
Source: NPS, 2023.

2. How would you rate the strength of other agencies you work with in regard to interagency cooperation?



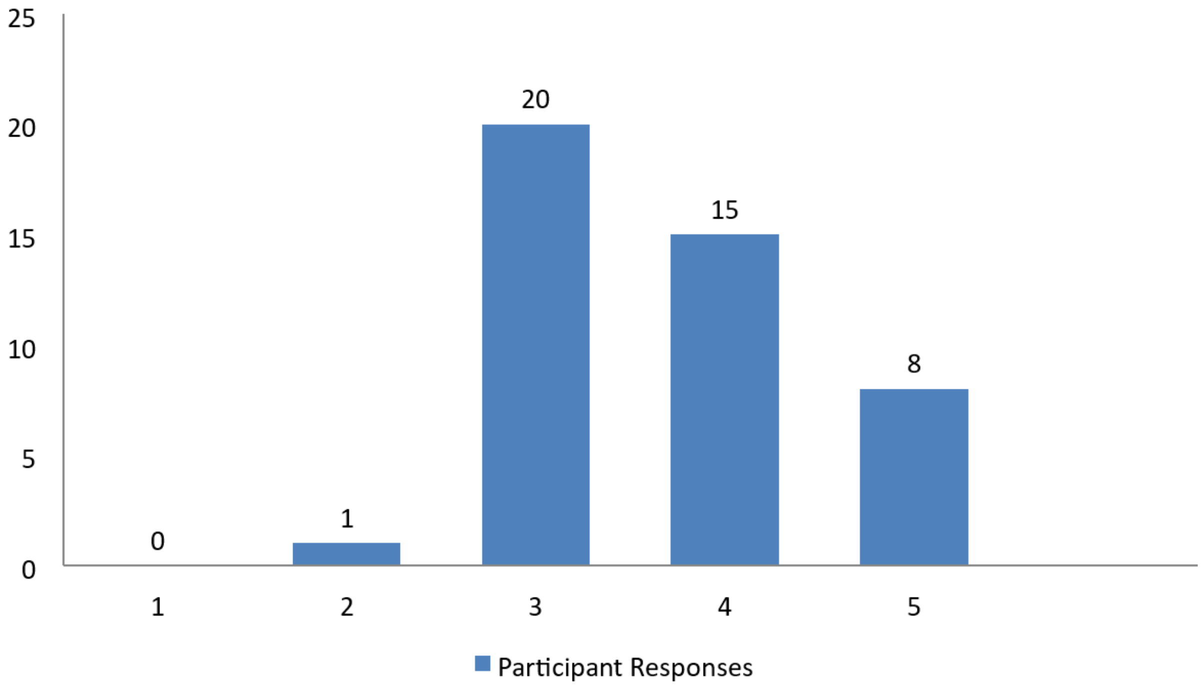
Source: NPS, 2023.

3. How would you rate the strength of your agency with regard to collaborating regionally?



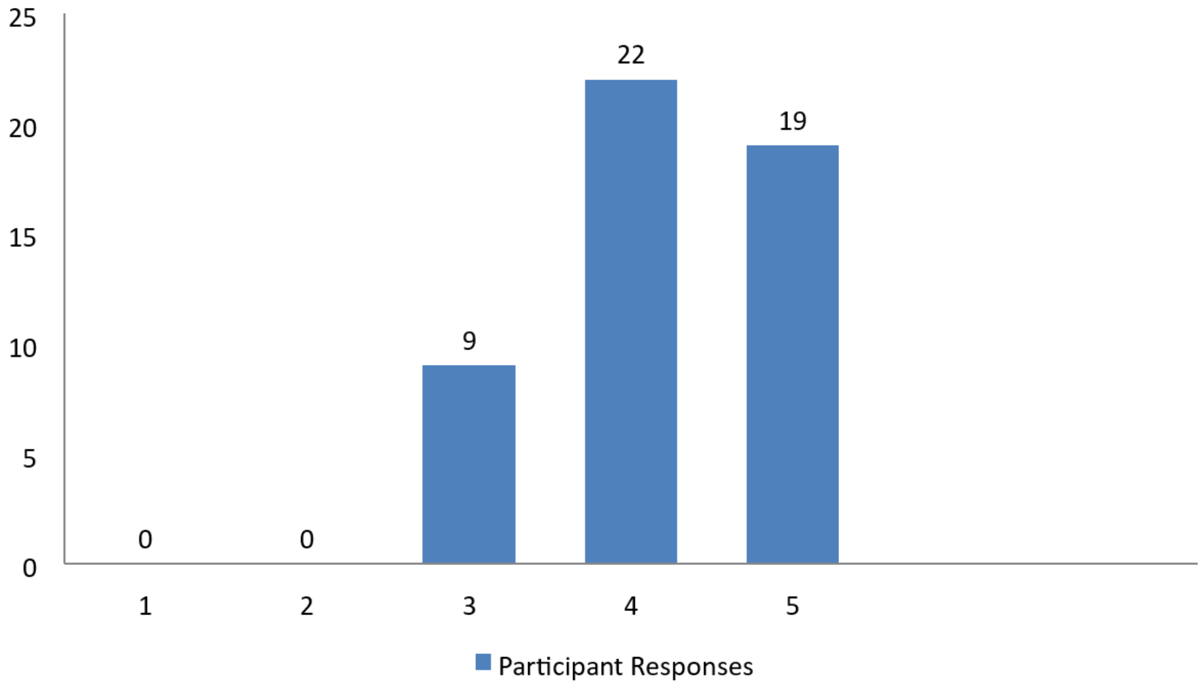
Source: NPS, 2023.

4. How would you rate the strength of other agencies you work with in regard to regional cooperation?



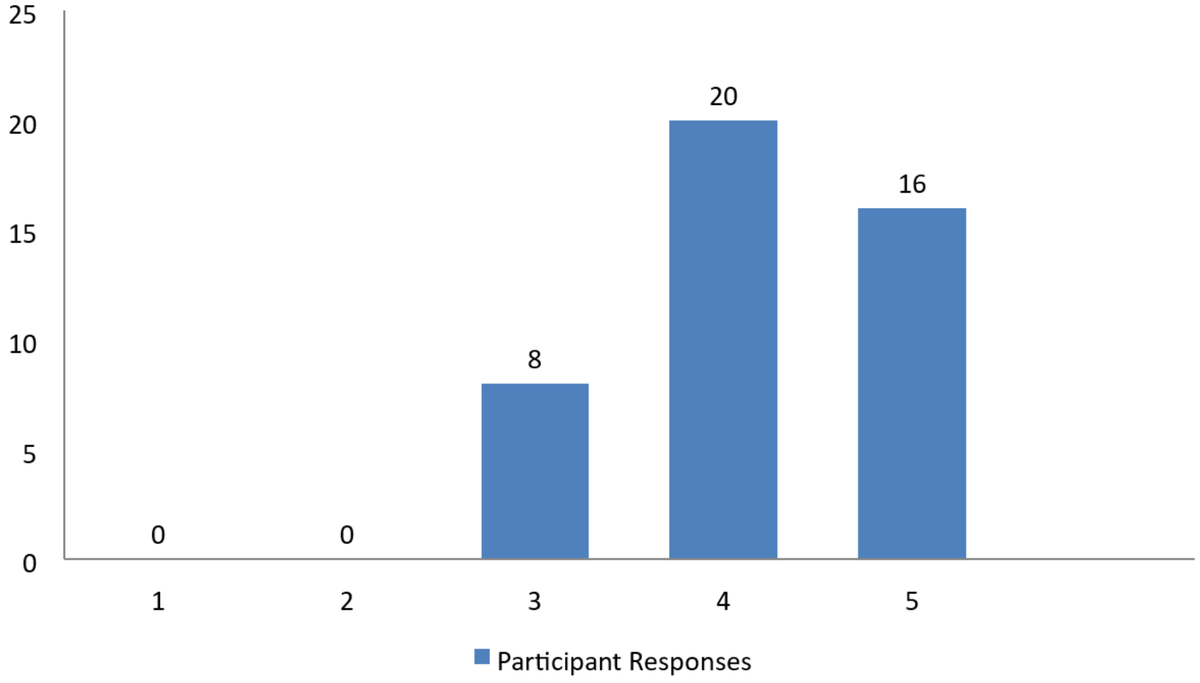
Source: NPS, 2023.

5. Do you believe the engagement helped your agency to strengthen their capability to enhance emergency planning, prevention, and threat response to incidents targeting Critical Energy Infrastructure?



Source: NPS, 2023.

6. After participating in this engagement, would you say your ability to support your agency in building resilience has increased?



Source: NPS, 2023.

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

— by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

— at the following standard number: +32 22999696,

— via the following form: european-union.europa.eu/contact-eu/write-us_en.

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

EU open data

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

Science for policy

The Joint Research Centre (JRC) provides independent, evidence-based knowledge and science, supporting EU policies to positively impact society

EU Science Hub
joint-research-centre.ec.europa.eu

Publications Office
of the European Union