European Commission

JRC TECHNICAL REPORT

Tabletop Exercise: Coherent Resilience Baltic 2021 (CORE 21-B)

Final Report

Nave C., Kopustinskas V., Dirginčius E., Walzer L., Beniulytė G., Purvins A., Masera M., Nussbaum D., Norg V., Užkuraitis D.

2022

CORE 21B

Joint Research Centre

EUR 31020 EN

Contact information
Name: Vytis KOPUSTINSKAS
Address: European Commission, Joint Research Centre (JRC),
via E. Fermi 2749, Ispra (VA), 21027, Italy
Email: vytis.kopustinskas@ec.europa.eu
Tel.: +39.0332.786257

EU Science Hub
https://ec.europa.eu/jrc

JRC128730

EUR 31020 EN

PDF	ISBN 978-92-76-49466-9	ISSN 1831-9424	doi: 10.2760/74397
Print	ISBN 978-92-76-49393-8	ISSN 1018-5593	doi: 10.2760/850219

Luxembourg: Publications Office of the European Union, 2022

How to cite this report: Nave C., Kopustinskas V., Dirgінčius 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.

Contents

Foreword

This report constitutes the final report of the CORE21-B Tabletop exercise, jointly 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 which also drafted the final report.

Acknowledgements

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

Syndicate 1 - STRATCOM: Mr. Aleksandras MATONIS (journalist, Lithuania)

Mr. Lukas TRAKIMAVIČIUS (NATO ENSEC COE)

Syndicate 2 - HYBRID-CYBER: Mr. Stefano BRACCO (ACER)

Mr. Mark PROUSE (UK, BEIS)

Syndicate 3 - Crisis Response: Mr. Julijus GRUBLIAUSKAS (NATO HQ)

Mr. Jeffrey PRINGLE (US DOE, US EUCOMM)

Syndicate 4 - Synchronization: Dr. Vytis KOPUSTINSKAS (JRC)

Ms. Jolanta ZAPKUVIENĖ (NATO ENSEC COE)

The Core Planning Team:

LTC Christophe NAVE (NATO ENSEC COE)

Dr. Vytis KOPUSTINSKAS (JRC)

CPT Evaldas DIRGINČIUS (NATO ENSEC COE)

Dr. Arturs PURVINS (JRC)

Ms. Ana GOGORELIANI (NATO ENSEC COE)

Ms. Greta BENIULYTĖ (NATO ENSEC COE)

Interaction Team:

LTC Christophe NAVE (NATO ENSEC COE)

Mr. Pawel KASPRZYK (HYBRID COE)

Dr. Sigita KAVALIŪNAITĖ (Ministry of Foreign Affairs of the Republic of Lithuania)

Mr. Markus METSALA (HYBRID COE)

Mr. Tomas ZIMNICKAS (LITGRID)

Ms. Ana GOGORELIANI (NATO ENSEC COE)

Mr. Viktoras PINKEVIČIUS (Ministry of Defense of the Republic of Lithuania)

LECTURERS:

Mr. Max BRANDT (European Commission, DG HOME)

Mr. Mark Prouse (UK BEIS)

Mr. Jan-Olof OLSSON (Swedish Civil Contingency Agency)

Dr. Justinas JUOZAITIS (Lithuanian Military Academy)

Mr. Vytautas BUTRIMAS (NATO ENSEC COE)

Dr. Vytis KOPUSTINSKAS (JRC)

The authors acknowledge excellent contribution of the TTX Evaluation group in collecting information for this report: CDR Chad Bollmann (USN, NPS), CDR Chad Brahler (USN Reserves), CDR Regis Dowd, (USN Reserves), Mr Alan Howard (NPS), CDR Ryan Hughes (USN Reserves), LCDR Kevin Jacobson (USN Reserves), LT Vikram Kanth (USN, NPS), LTC Peter Katzfey (USA, JFC-Brunssum), CDR James Klonski (USN Reserves), LTC Cindy LeGarie (Can), Mrs. Rebecca Lorentz (NPS), Dr. Ryan Maness (NPS), CAPT Mark Murphy (USN Reserves), Dr. Daniel Nussbaum (NPS), Mr. Mark Petri (US DOE Argonne National Laboratory), CDR Heath Rasmussen (USN Reserves), CDR Sheila Sklerov (USN Reserves), Capt. Robert Stelmack (NPS, USAF), Mr. Lawrence M. Walzer (NPS), LCDR Stephen Winchell (USN Reserves), and CAPT Jon Young (USN Reserves).

Authors

Christophe Nave, Vytis Kopustinskas, Evaldas Dirginčius, Lawrence M. Walzer, Greta Beniulytė, Arturs Purvins, Marcelo Masera, Daniel Nussbaum, Videt Norg, Darius Užkuraitis

Abstract

Coherent Resilience 2021 – Baltic (CORE 21-B) was a Tabletop Exercise (TTX) 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 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. 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 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.

1 INTRODUCTION

1.1 Coherent Resilience Program

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. Coherent Resilience 2021 - Baltic (CORE 21-B) was the second 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 CORE21-B follows excellent feedback and experience gained during execution of CORE-19 TTX (Kopustinskas et al., 2019).

1.2 Coherent Resilience 2021 Baltic (CORE 21-B)

1.2.1 Overview

CORE 21-B was a TTX 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 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 (**Figure 1**). **Table 1** in Annex 1 captures the list of participating organizations.

The CORE 21-B TTX was prepared in a series of preparatory meetings in Vilnius, Lithuania in person, virtually or in hybrid format – 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).

Figure 1. CORE21-B Participants «Family Photo»

Source: NATO ENSEC COE, 2021.

1.2.2 Purpose, Aim, Objectives

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 Astravets 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 (Hybrid CoE, 2019) 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 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.

1.2.3 Concept for the Event

CORE 21-B was opened by welcome messages of COL Darius Užkuraitis, Director of NATO ENSEC COE (**Figure 2**) and Dr. Habil. Piotr Szymański, Director of Directorate C of the JRC (**Figure 3**).

Figure 2. Col. Darius UŽKURAITIS, Director of NATO ENSEC COE, provides welcoming remarks

Source: JRC, 2021.

The TTX was divided into three phases that included an academic seminar, the tabletop exercise, and the distinguished visitors' day/after action session.

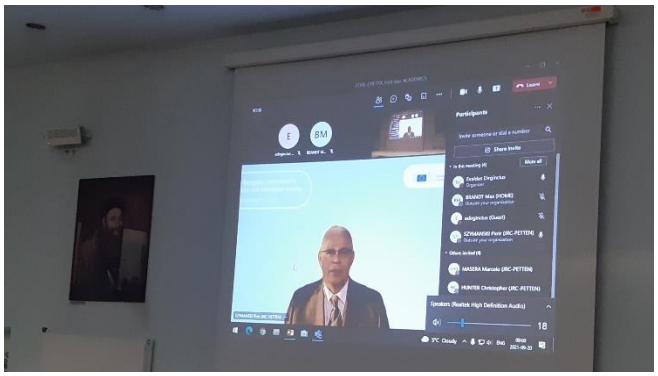
Phase One, the academic seminar consisted of a series of expert presentations to better prepare participants for the TTX. Lectures included the following topics: EU Initiatives for Resilient Critical Infrastructure, presented by Max Brandt (DG HOME); Hybrid Threats from UK Perspective, presented by Mark Prouse (UK Government, BEIS); Crises management in a utility during a blackout, presented by Jan-Olof Olsson (Swedish Contingency Agency); Belarusian NPP: Impact to the Neighborhood, presented by Dr. Justinas Juozaitis (Lithuanian Military Academy); Cyber Threats Impact to Critical Industrial Infrastructure, presented by Vytautas Butrimas (NATO ENSEC COE); a series of Transmission System Operator (TSO) presentations from ELERING, AST, LITGRID, and Svenska Kraftnat; the TTX Scenario Presentation by LTC Christophe Nave (NATO ENSEC COE); and a presentation of the Baltic power grid simulations by Dr. Vytis Kopustinskas (JRC).

Phase Two of CORE 21-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) Strategic Communications (STRATCOM), (2) Hybrid-Cyber, (3) Crisis Response, and (4) Synchronization. Each syndicate had two Co-Facilitators to lead discussions and a small cell of evaluators. Each syndicate also had a representative of an Interaction Team, which was a

new CORE program initiative designed to support information sharing between the syndicates during the execution of the TTX.

Phase Three of CORE 21-B consisted of the TTX After Action (Hot Wash) and coincided with the Distinguished Visitors' Day held at the Presidential Palace of the Republic of Lithuania. 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 participants were addressed by Mr. Darius Kuliešius, Chief Advisor for National Security to the President of Lithuania.

Figure 3. Dr. Habil. Piotr SZYMAŃSKI, Director of the Directorate C of the JRC, provides opening remarks remotely



Source: JRC, 2021.

1.2.4 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 with the exercise scenario, then provides a separate section for each syndicate where the vignettes and injects are followed by a summary of the syndicates' responses. 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, so syndicate responses are completed in line with the scenario, but 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 from 11-12 November 2021, where several facilitators, participants, and evaluators gathered to develop much of the final content of this report – it was a team effort.

2 CORE 21-B Tabletop Exercise

2.1 Structure of Vignettes and Injects

What is a vignette? Typically, vignettes provide a high-level overview describing a significant crisis situation used to illustrate or identify a particular issue. 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? 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).

The training audience will discuss four vignettes and a number of injects for each vignette within 4 syndicates:

Syndicate 1 – STRATCOM

Syndicate 2 – Hybrid-Cyber

Syndicate 3 – Crisis Response

Syndicate 4 – Synchronization

2.2 Syndicate 1 – Strategic Communications (STRATCOM)

The syndicate work view is shown in **Figure 4**.

Figure 4. Syndicate 1 - *Strategic Communications* in discussions

Source: NATO ENSEC COE, 2021.

Key Takeaways and Recommendations

Expand upon existing National Crisis body with STRATCOM. The Baltic States already demonstrate a robust capability for the creation of a National Crisis body in response to rapidly evolving and dynamic threats and emergencies. However, a standard documented process does not exist for the utilization and elevation of STRATCOM management in an emergency scenario. Syndicate members discussed several times how attribution is key in their messaging and wanted to wait for definitive attribution. The problem here is that attribution in hybrid actions can sometimes take weeks if not longer. **Recommendation**: Establish protocols to assess risk, coordinate responses, and organize efforts within the existing National Crisis body in order to quickly and effectively execute response narratives to any emergency or hybrid threat. Strategic communication in response to adversary operations will often-times be dependent upon attribution of the actor. Because attribution can take a lengthy amount of time, it is important that STRATCOM is able to leverage existing evidence in a timely manner to include hinting at likely actors prior to official attribution. In the scenario, it was observed how Russia and their allies could do this by having a "reporter" ask the pointed question and then by giving a non-committal answer that "we have not ruled out any suspect."

Establish a Joint Baltic STRATCOM Process. Currently there is no standardized process for joint, synchronized, and cohesive development and execution of STRATCOM between the three Baltic States. Current processes would vary between types of STRATCOM and situations, adding additional friction when time and expertise are relevant factors. In some scenarios, there were events affecting the power grid in all three of the Baltic States that would seem minor when viewed in isolation, but when put together painted a much more significant picture. Members of the syndicate pointed out that they did not have the level of communication that would enable them to know about all of these issues in the other countries. It often took until each nation had identified enough events within their own borders before they reached out to each other. Members would point out how the same messaging wouldn't work for each Baltic State and how even within their nations they have different minority groups and different age groups, and that one message cannot cover everyone. They were very aware that minority groups can feel even more vulnerable during a crisis and that it is important to reach out to them appropriately. **Recommendations:** Establish a Joint Baltic STRATCOM process, ranging from the development of consistent points of contact for synchronizing STRATCOM to the establishment of a standing Joint Baltic STRATCOM organization. In areas that affect the Baltic States and their partner nations, such as

synchronization, there needs to be more communication at every level. The power companies of the Baltic States, Sweden, Poland, and Finland should have more robust communications amongst themselves. There also needs to be an increase in communications between all of the nations involved at a high enough level (Minister of Energy or equivalent) to allow for the potential to identify patterns across borders that could signal ongoing hybrid operations. As long as the messaging supports the narrative, it does not have to be exactly the same. It is important to put it out via every language possible for internal and international control of the narrative. As part of this, there are a multitude of media types now and their usage often varies with age and culture. It is important to tailor the narrative to fit each type of media to ensure maximum coverage.

Elevate the importance of external STRATCOM. Throughout the scenario Russia would use messaging, sometimes via Belarus or Kaliningrad social media and news networks, in conjunction with its operations to increase the impact the operations would have on the image of the Baltic States to their citizens and the international community. Oftentimes, members of the syndicate would just state that, "Russia does these kinds of statements all of the time, there is no need for us to respond to them," thereby allowing Russia's propaganda to influence the overall narrative. Furthermore, the exercise team was correctly focused on internal messaging to their citizens as a priority during the various crises presented in the exercise. One of their key realizations during the exercise was the need to do a better job today in communicating to the Russian-speaking ethnic minorities within the country. The additional external audiences of allies and of the aggressor were sometimes missed, however. **Recommendation**: Identify channels and institute ongoing messaging in Russian to the Russian-speaking citizenry, so that this is established and available for use during a crisis. Establish response protocols that include all three (domestic, international, adversarial) audiences so that allies and the aggressor are included in communication planning. Develop partnerships with news stations and social media influencers e.g. "internet elves" to allow for each nation to respond to Russian propaganda in situations in which an official press release is not warranted. Each Baltic State needs to have a social media team as part of their strategic communications team that will counter Russian propaganda at the appropriate level in a way that helps further the overall strategic narrative for their nation.

Standardize National STRATCOM Processes. STRATCOM personnel did not have access to previously established strategic narrative guidance, and the process of getting a form of that guidance from supranational organizations was slow and ineffective. Further, there does not exist a standardized process for coordinating STRATCOM across Lithuanian municipalities. The absence of a standardized process increased the time it took to perform STRATCOM and therefore reduced or eliminated its effectiveness, especially in regards to combatting foreign misinformation. The two in conjunction pose a threat to the effective use of STRATCOM in a crisis situation. **Recommendations:** 1) Develop a long-term strategic narrative for each key issue such as synchronization. 2) Ensure STRATCOM personnel have access to the crisis management personnel. Since speed is vital for maintaining control of the narrative, develop protocols and pre-approved messaging themes that can automatically be released for a variety of emergency situations. 3) Establish a common method for synchronizing STRATCOM amongst municipalities. A crucial part of messaging is not just in asking for help, but in letting one's citizens know what help is expected locally and when.

Identify existing and required capabilities and integrate into STRATCOM planning. STRATCOM syndicate members sometimes could not gather information on what additional capabilities were required (e.g., spare parts and technicians for power stations, naval assets to shadow and track Russian activity off the coast), what assets NATO members, the EU, partner nations, and international organizations have in inventory, and an understanding of time/distance for the requested capabilities/aid to arrive in the area of operations. This lack of on-demand technical information resulted in delays of STRATCOM execution. **Recommendations**: In preparation for coordination amongst the Baltic States, NATO, the EU, partner nations, and international organizations, the Baltic State governments should identify existing capability and capacity gaps to secure critical infrastructure and supply chains and include the stakeholders in the national crisis management plans, policies, and procedures. This information should then be integrated to the existing STRATCOM structure so that they're able to leverage technical information, resulting in their operations becoming more timely and effective.

2.3 Syndicate 2 – Hybrid-Cyber Security

The syndicate work view is shown in **Figure 5**.

Figure 5. Syndicate 2 - Hybrid and Cyber Security team in discussions

Source: NATO ENSEC COE, 2021.

Key Takeaways and Recommendations

Hybrid Uncertainty Requires New Considerations and Processes. The timeline of identifying and confirming stealthy cyber attacks cannot be reconciled with critical infrastructure service requirements; it can take up to 9 months to confirm a cyber attack on operational technology (OT) equipment and 12 months to acquire replacement equipment such as transformers. Restoring the software backups for only one substation was estimated to take 24 hours. Meanwhile, to mitigate the most severe impacts, TSOs must restore and resolve outages in power and many other services on a scale of hours or less. **Recommendation(s):** Governments and critical infrastructure (CI) operators should evaluate existing regulations and processes to validate responsiveness to hybrid threat scenarios and discuss concerns at the cross-organizational and national level. New skill and resource sharing agreements may improve resiliency to hybrid threats. Inter-national regulations, cross-functional team compositions, and cross-border linkages should also be evaluated for effectiveness against hybrid scenarios. For instance, Lithuania (and possibly other states) does not have a legal definition of a "hybrid threat" and "hybrid attack"; however, legally defining the term may narrow the scope of "hybrid threat" and "hybrid attack" and permit defining thresholds for precise and rapid crisis response. There may be additional benefit from examining practices, policies, and regulations across the EU. Related, Baltic States should review drone policies with respect to critical infrastructure and add illegal drone operations and hybrid drone attacks to ongoing exercises. Mutual aid agreements (e.g., sharing of experts or key assets such as step-down transformers) can improve regional resiliency and mitigate short- and medium-term impacts. Operational testing at the component and system level, including restoring systems from backup and specialized red-teaming, can aid in the identification and mitigation of vulnerabilities to systemic advanced cyber attacks at national or regional scales. These inter-organizational linkages, policies, and procedures are other components of a hybrid security culture.

Syndicate 2 Best Practices

Cooperation and Coordination. Massive information sharing among all Baltic region stakeholders in the electricity sector is ongoing but can be improved. Enhance analysis capabilities of the market operators in respect to hybrid threats. Consider opening a communications channel between intelligence and sector operators. Electricity System Operators coordination and cooperation is the ideal Best Practice. **Strengths**: Close cooperation and coordination among Baltic States is common practice.

Establishing a Culture of Hybrid Threat Awareness. As the first steps towards establishing a "culture of hybrid threat awareness," LITGRID has been experimenting with automating and aggregating field equipment trouble reports at the operations center. Additionally, they have conducted training exercises designed to sensitize field engineers and managers to alert and report potential indicators of cyber/hybrid attack. Estonia reported that this aggregation capability is also under development. **Recommendation:** Consider adopting the same system in all other Baltic Region countries. Aggregated reporting and sensitization could enable more rapid and effective response.

Regulation on risk preparedness in the electricity sector. Working on the implementation on the adopted EU regulation, EU nation states must coordinate a risk preparedness plan. National plans that are being prepared are projected to be signed in January of 2022. These plans are established and then tested by TSO together with their national competent authorities. **Recommendation:** Make an extensive use of solidarity clauses through the use of existing regulations. Use of multinational/regional exercises as Coherent Resilience to continue to establish proper cooperation and coordination.

Emergency Communications. As it pertains to internal DSO/TSO procedures, ministries and institutions manage electricity supply crises communications via e-mail, phones, and cellphones. **Recommendation**: Usage of military equipment as backup communication as needed in order to enhance resilience of the underlying telecommunication system of the energy grid. Alternatively, establish a reliable centralized control center to manage emergency communication in the Baltic region.

Cross-check essential information. To have in place a system for information sharing on hybrid threats involving all Baltic States. **Recommendation:** To develop capabilities across national organizations and among the Baltic States to reconcile and cross-check designated essential elements of information, such as failures in critical equipment, cyber attack signatures and methodologies, and other potential indications of hybrid attack.

Checklists in Eventuality of a Cyber Incident on TSO/DSO. During a potential cyber incident at a TSO/DSO, which can have a very serious consequences for electrical power regulation in the network, appropriate authorities including ministry agencies and CERT are to be notified. The Syndicate highlighted existing systems that allow information sharing between TSO/DSOs and agencies including CERT. In this type of situation, a checklist exists to determine who should be contacted at the appropriate agencies in this type of event and in what order. **Recommendation**: Make good use of existing checklists and extend their scope to hybrid threats.

2.4 Syndicate 3 – Crisis Response

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

Figure 6. Crisis Response Syndicate 3 in discussions

Source: NATO ENSEC COE, 2021.

Key Takeaways and Recommendations

No larger coordination mechanism (forum) and battle rhythm for information flow across Baltic States. Shared lessons learned and best practices do not get captured and reviewed from previous experiences. Transmission System Operators (TSOs) communicate well across the Baltic States, however, the various governmental agencies do not have good information flow for sharing issues and lessons learned. This impedes timely coordination, continued learning, and improvement across all Baltic States. There is some informal coordination, however, there is no designated forum or regular battle rhythm for meeting. **Recommendation:** Establish an inter-state forum for sharing crisis response related issues and best practices on a recurring schedule. Establish a method for better communication between government institutions via official institutional representatives that coordinate with each other during crisis.

Need for greater coordination between civil defense, specifically, emergency responders at national and regional levels. Close coordination is required with the civil defense and emergency responders to identify and assist vulnerable populations during power outages. Coordination is required at local-national-regional levels. Although there is much done at the TSO level, there is currently no coordinated Baltic State crisis management mechanism at the government level. Information flow between various ministries is impeded due to differences in roles and responsibilities across the Baltic States (e.g. Cyber responsibility is in different ministries across each Baltic State) causing some issues in coordination. **Recommendation:** Establish lines of communication for coordination and define each Ministry and other institutions' roles. Leverage the inter-state forum mentioned previously. Establish a regional restoration assistance mechanism in order to enable the quick restoration of transmission lines. Consider establishment of a 3B regional crisis management mechanism.

No means for communicating threats and coordinating responses when internet and telecommunications are down. There is no plan across the Baltic States to maintain critical communications during a crisis when the communication infrastructure is down. TSOs can communicate between themselves, however, not with the government and consumers. **Recommendation**: Consider access of TSO representatives to secure government communication. Consider options for alternative communication lines such as UK military deployable satellite type communications, satellite phones, and Terrestrial Trunked Radio.

Lack of long-term preventive measures addressing vulnerabilities. Critical infrastructure is vulnerable to kinetic attacks, such as drone strikes, car bombs, and plane crashes, which can cause power outages. There is no plan for protection against attacks by state and non-state actors. **Recommendation**: Mitigation measures should be implemented to address vulnerabilities such as maintaining a running list of vulnerabilities and conducting regular reviews. Prioritization of critical infrastructure needs to be held centrally by the government. Upgrading physical security measures and conducting appropriate training is crucial for ensuring security of critical infrastructure. Exchange best practices between security providers and government agencies (armed forces, law enforcement, and intelligence agencies).

Procedures needed for fuel distribution from reserves in case of power outage. It is unclear if current procedures are adequate to facilitate distribution of fuel for power generators during a crisis. Storage and stock levels for fuel reserves and other supplies need to be reviewed and updated on a regular basis. Contracts should be established for fuel storage and distribution logistics such as acquisition, delivery, and security. **Recommendation**: Review and update contracts for fuel distribution and storage on a regular schedule. Evaluate procedures regularly for accuracy and efficiency.

Continuity for Operations Planning (COOP) for Government TSOs have developed plans and have exercised them. In addition, the Latvian Ministry of Defense crisis response exercise involves other government and municipal representatives. There are also Business Continuity Plans in place for Lithuania government to perform their functions from alternative locations outside the 100 km radius from the Belarusian NPP. **Recommendation:** These plans should not conflict with other crisis response plans. Connectivity between alternate sites for government continuity should be tested on an annual basis and it should be ensured that there is sufficient space for critical government workers to perform their duties. Appropriate institutions should develop coordinated evacuation plans for critical governmental agencies; create standardized SOPs for communication and action during emerging crisis such as cyber/hybrid attack; and develop an annual requirement to review and exercise COOP for critical government services.

2.5 Syndicate 4 – Synchronization

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

Figure 7. Syndicate 4 - Synchronization in discussions

Source: JRC, 2021.

Key Takeaways and Recommendations

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 GHG emission technologies should be analyzed for feasibility.

Improve resiliency of gas-fired power generation. In the case of decreased capacity on inter-connectors and low renewable energy supplies, the Baltic States rely on gas power generation. There is a need in the Baltic States to ensure resilient gas-fired power plants as these are among the few baseload generation sources currently available. **Recommendation:** It is recommended to analyze and implement additional measures to ensure resilient generation from natural gas power generation: including redundant pipeline supply options, ensuring dual-fuel possibility and fuel availability on-site, regional diverse supply options, and gas storage.

Clarified load-shedding procedures would make system restoration processes more clear. When power imbalances exist and generation options are limited, system operators need to issue load-reduction instructions. Demand-response programs send market signals to incentivize consumers to reduce consumption. Programs can be implemented to pay major industry and commercial customers (at both the transmission and distribution level) to reduce consumption upon notification from the power supplier. It is important to clarify load-shedding processes and procedures. There are currently legal implementation and procedure implementation gaps amongst Baltic nations such as in the case of system restoration procedures as some logistical details require additional clarification. Such programs are highly effective in reducing demand during peak hours or emergencies and add significant flexibility to system operators in their response actions. **Recommendation**: Load-shedding procedures need to be enhanced at TSO and DSO level. The region should consider the possibility of preemptive contracted load shedding in one country to sustain operations in another Baltic country.

There should be an establishment of a duty officer to coordinate communications during emergency situations. Some transmission system operator companies appoint a duty officer during severe events who is responsible for communicating with outside entities including federal authorities, in-country response agencies, and out-of-country partners such as the use of foreign support crews. This person coordinates joint activities

of the TSO with those external groups for the duration of the crisis. Currently there is no such position within the Baltic TSOs. **Recommendation**: It is recommended that each of the Baltic TSOs establish this role within their organization. This would remove some of the communication burden from dispatchers as well as benefiting the decision-making process by facilitating communication between response agencies.

There is limited flexibility in power system restoration options. There are a limited number of restoration-based scenarios. For power system restoration, there are a lack of alternatives. Having more options would make the restoration process more resilient to unexpected issues which may arise following standard procedures. **Recommendation:** Consider amending current instruction to increase the number of power system restoration options.

There are currently no structured means to communicate threats and coordinate responses when internet and telecommunications are down. There is no plan across the Baltic States to maintain critical communications during a crisis when the communication infrastructure is down. TSOs can communicate between themselves, however, not with the government and consumers. **Recommendation:** Consider access of TSO representatives to secure government communications. Consider options for alternative communication lines such as UK military deployable satellite type communications, satellite phones, and Terrestrial Trunked Radio.

A flexible adaptation of shifts of operational staff can increase efficiency in emergencies. Emergencies are inherently stressful situations, increasing the likelihood of missteps that can worsen the crisis. The probability of mistakes increases significantly when responders are overworked and tired. Some TSOs have adopted shortened emergency shifts for operational staff (e.g., three- hour shifts) during emergency operations. Every half hour there is a 2-minute check-in to ensure that the team is aligned on the unfolding situation and needed actions. This schedule is maintained even if it means housing multiple shifts at one location. **Recommendation**: It is recommended that the Baltic States TSOs adopt a policy supporting flexible shifts of operational staff during emergencies. This would allow the operational staff to be more efficient and minimize the likelihood of error.

3 Concluding Exercise Key Takeaways and Recommendations

The following key takeaways and recommendations are those identified by the broader syndicate teams that consisted of facilitators, participants, and evaluators who collaborated on the developed syndicate reports consolidated within chapter 2 with topics that were beyond their specific syndicates captured below.

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 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. As part of this service, include a government sponsored initiative for emergency radios (battery powered, hand-wound) among the citizen population. Increase coordination and develop a standardized process for interaction between the different levels of government (national, municipality, and city) concerning emergency communications to the population and information exchange to maintain better situational awareness at every

level during an emergency. 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 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.

4 Concluding remarks

It is important to note that this report – ideally – does not end CORE21-B, for the region, nations, departments, and organizations that participated in the TTX should each develop an Improvement Plan based on the relevant key takeaways identified. Each state or institution is to further analyze the key takeaways pertinent to their organizations in order to identify the best means to facilitate improvements and develop the corresponding plan of action to make such positive changes in order to improve the effectiveness and efficiency of their organizations' responses to challenges related to critical energy infrastructure and hybrid threats – such a product would constitute their Improvement Plan. Lastly, the ENSEC COE has developed an initiative to reach out to CORE participants at various points in the future (six months, one year, etc.) to survey participants on any improvements that were implemented based on what was learned from CORE21-B.

Figure 8. Syndicate presentations for the guests of the Distinguished Visitors Day

Source: JRC, 2021.

Figure 9. Chief President Advisor Darius Kuliešius addresses the audience of the CORE21-B Distinguished Visitors Day at the Lithuanian President's Palace

Source: JRC, 2021.

Figure 10. Col Darius UŽKURAITIS provides welcoming remarks for the guests of the Distinguished Visitors Day at the Lithuanian President's Palace

Source: JRC, 2021.

Figure 11. Dr. Habil. Piotr SZYMAŃSKI provides opening remarks for the guests of the Distinguished Visitors Day at the Lithuanian President's Palace

Source: JRC, 2021.

Figure 12. Dr. Daniel NUSSBAUM, Director of NPS Evaluation Group discusses the final evaluation report during the Distinguished Visitors Day

Source: JRC, 2021.

References

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

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 978-92-76-11829-9, doi:10.2760/010525, JRC118083.

List of abbreviations and definitions

ACER	EU Agency for the Cooperation of Energy Regulators
B2B	Back to Back
BRELL	Belarus-Russia-Estonia-Lithuania-Latvia
CBRN	Chemical, Biological, Radiological and Nuclear
CORE	Coherent Resilience
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CHP	Combined Heat and Power
CISA	Cybersecurity and Infrastructure Agency
DSO	Distribution System Operator
ENSEC COE	Energy Security Centre of Excellence
EC	European Commission
ERAA	European Resource Adequacy Assessment
GHG	Green House Gas
HAPP	Hydro-Accumulating Power Plant
IAEA	International Atomic Energy Agency
ICS	Industrial Control System
IOC	Indicators of Compromise
IPS/UPS	Integrated Power System/Unified Power System
JRC	Joint Research Centre
MoD	Ministry of Defense
NIS	Network and Information System
NPP	Nuclear Power Plant
NPS	Naval Postgraduate School
TSO	Transmission System Operator
TTX	Tabletop Exercise
UCTE	Union for the Coordination of the Transmission of Electricity

List of figures

List of tables

Annexes

Annex 1: Participating Organizations

Table 1. List of participating organizations.

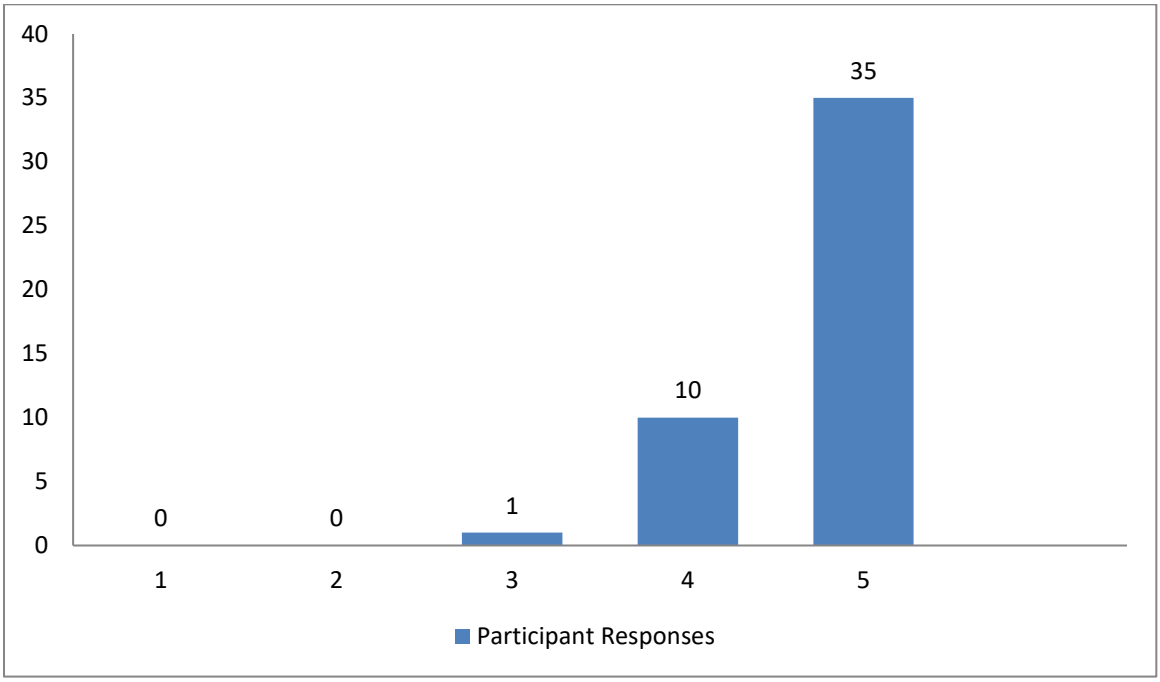
	Participating Organizations
1.	Svenska Kraftnät (Swedish TSO)
2.	Naval Postgraduate School (USA)
3.	Estonian Competition Authority
4.	The European Centre of Excellence for Countering Hybrid Threats (FI)
5.	Ministry of Foreign Affairs (LTU)
6.	Fingrid Oyj (Finish TSO)
7.	JFC Brunssum (NATO)
8.	Estonian Information System Authority
9.	SHAPE (NATO)
10.	Ministry of National Defence (LTU)
11.	National Energy Regulatory Council (LTU)
12.	Swedish Civil Contingencies Agency (SWE)
13.	Litgrid AB (LTU)
14.	Ministry of Economic Affairs and Communications of Estonia
15.	NATO Energy Security Centre of Excellence
16.	Ministry of Energy of the Republic of Lithuania
17.	Public Utilities Commission of Latvia
18.	UK Department for Business, Energy and Industrial Strategy (BEIS)
19.	NATO Strategic Communication Centre of Excellence
20.	Elering AS (Estonian TSO)
21.	Augstsprieguma tikls (Latvian TSO)
22.	Ministry of Economics Republic of Latvia
23.	EPSO-G (LTU)
24.	European Commission, Joint Research Centre
25.	Ministry of Economic Affairs and Communications of Estonia
26.	AB "Ignitis grupė" (LTU)
27.	Polskie Sieci Elektroenergetyczne (Polish TSO)
28.	National Energy Regulatory Council (LTU)
29.	NATO HQ
30.	US Department of Energy and US European Command
31.	Ministry of Defense of Republic of Latvia
32.	ACER (EU)
33.	Mission of Finland to NATO
34.	National Cyber Security Center under MoD (LTU)
35.	Lithuanian Energy Agency

Source: ENSECCOE, 2021.

Annex 2: Results of Participant Exercise Evaluation Surveys performed by NPS

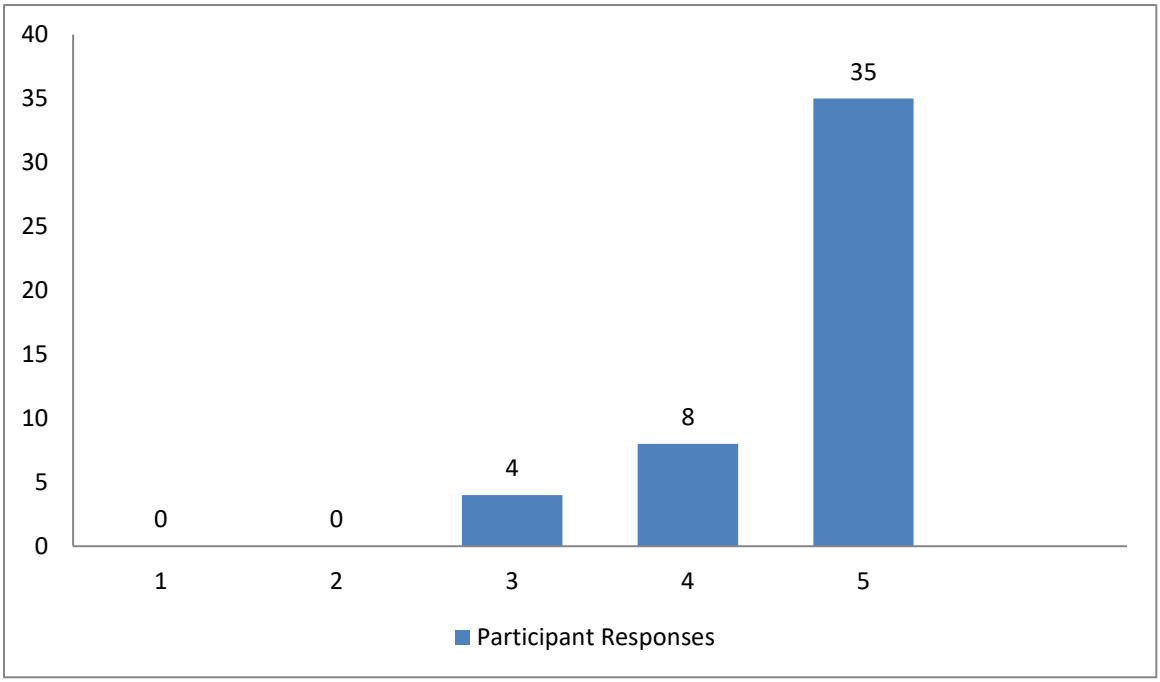
Quantitative Response Part I

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



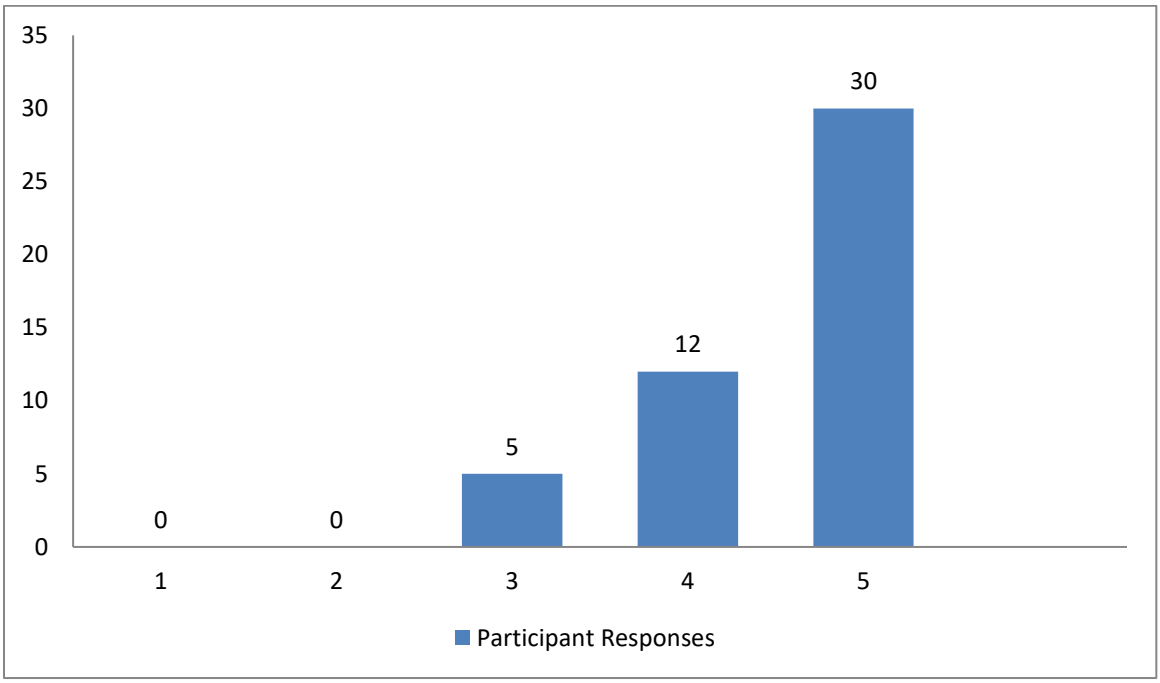
Source: NPS, 2021.

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



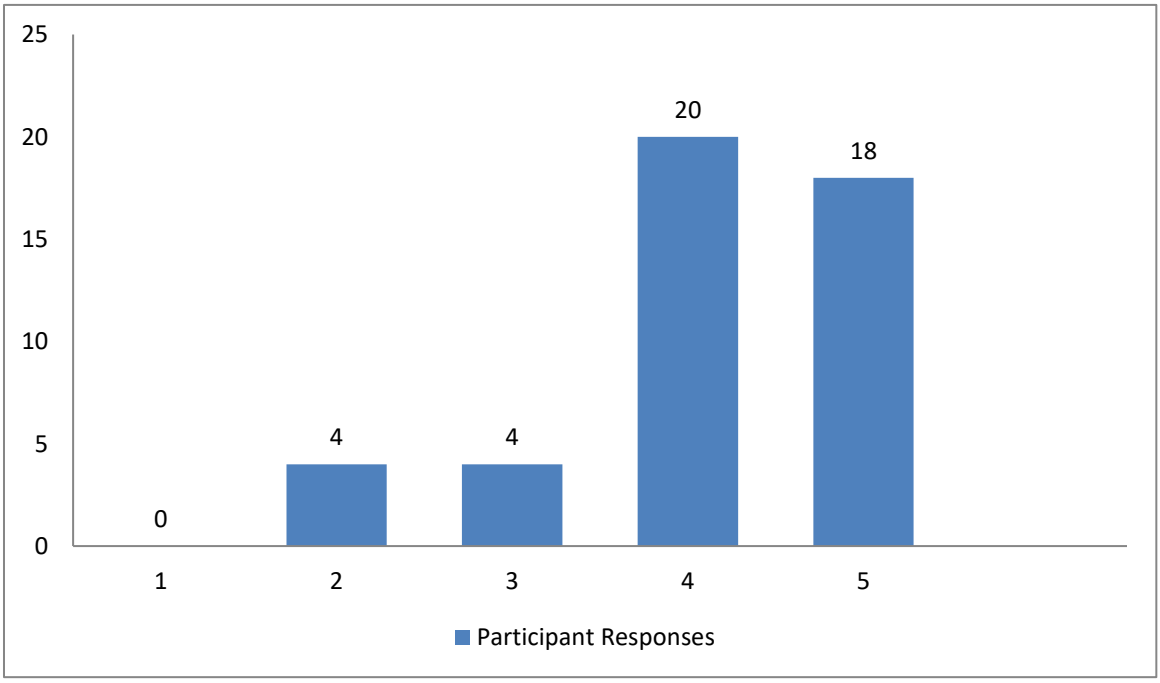
Source: NPS, 2021.

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



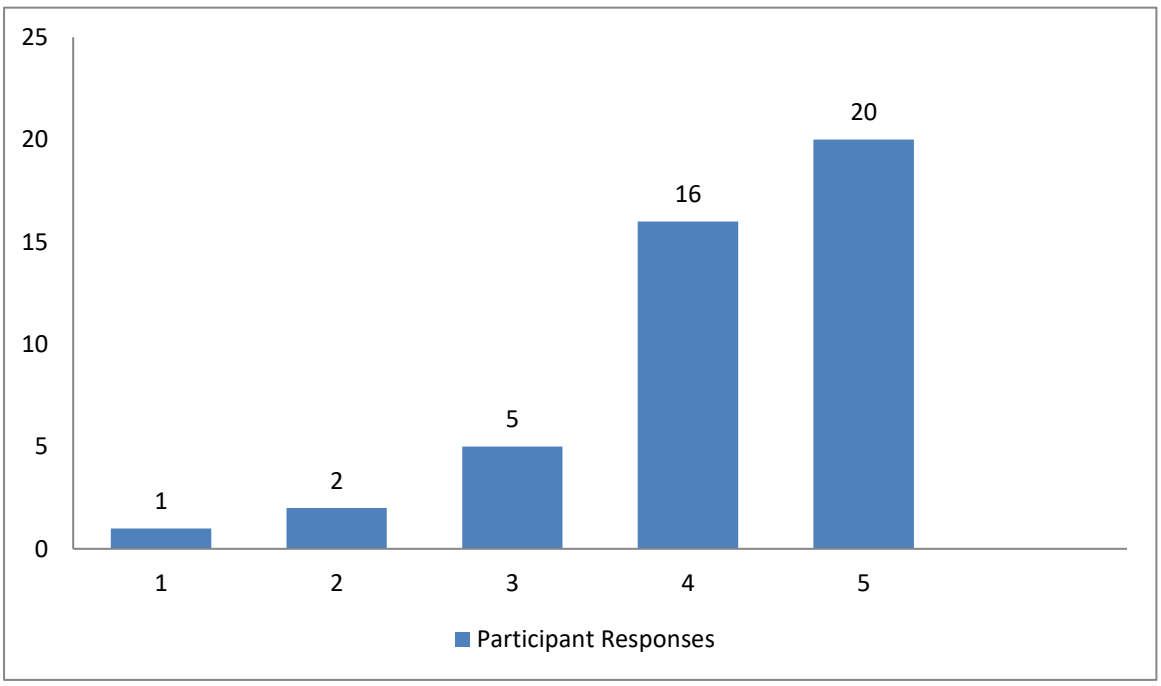
Source: NPS, 2021.

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



Source: NPS, 2021.

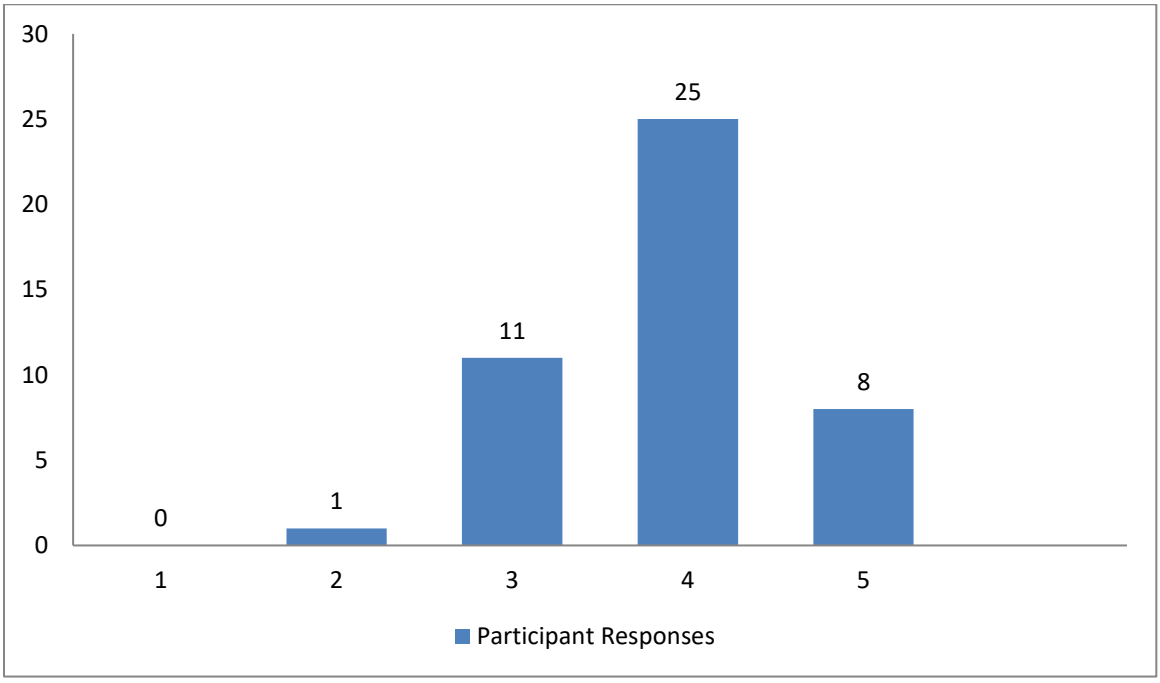
5. Participation in CORE TTX would be beneficial to my colleagues were they able to attend.



Source: NPS, 2021.

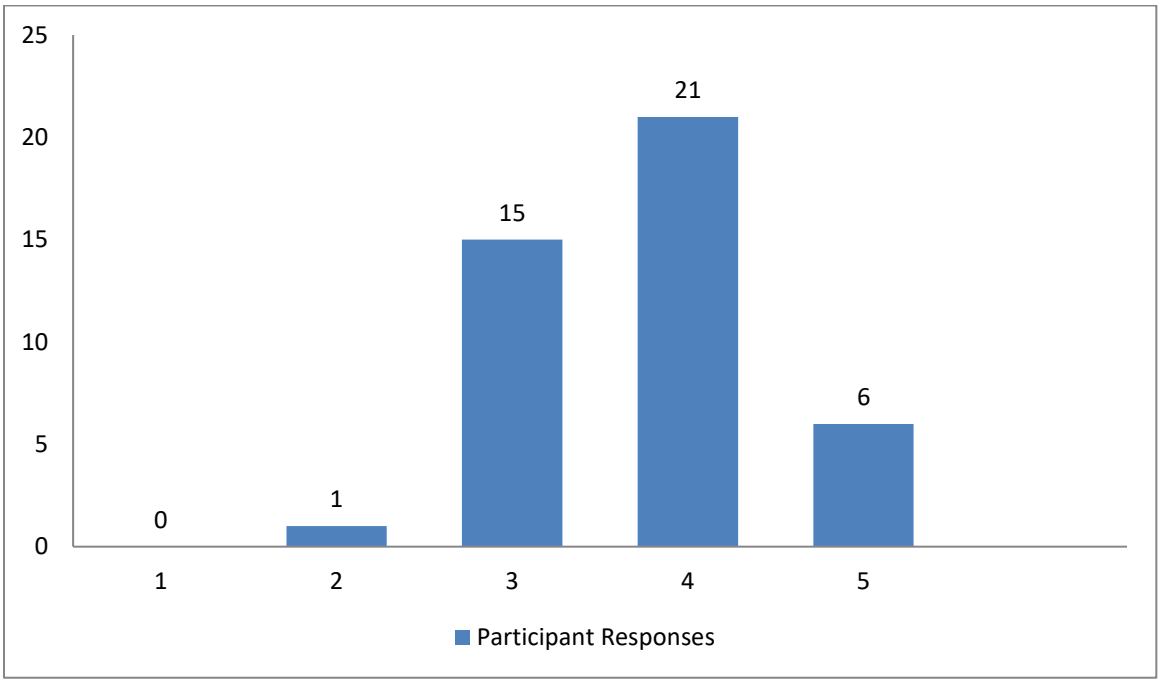
Quantitative Response Part 2

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



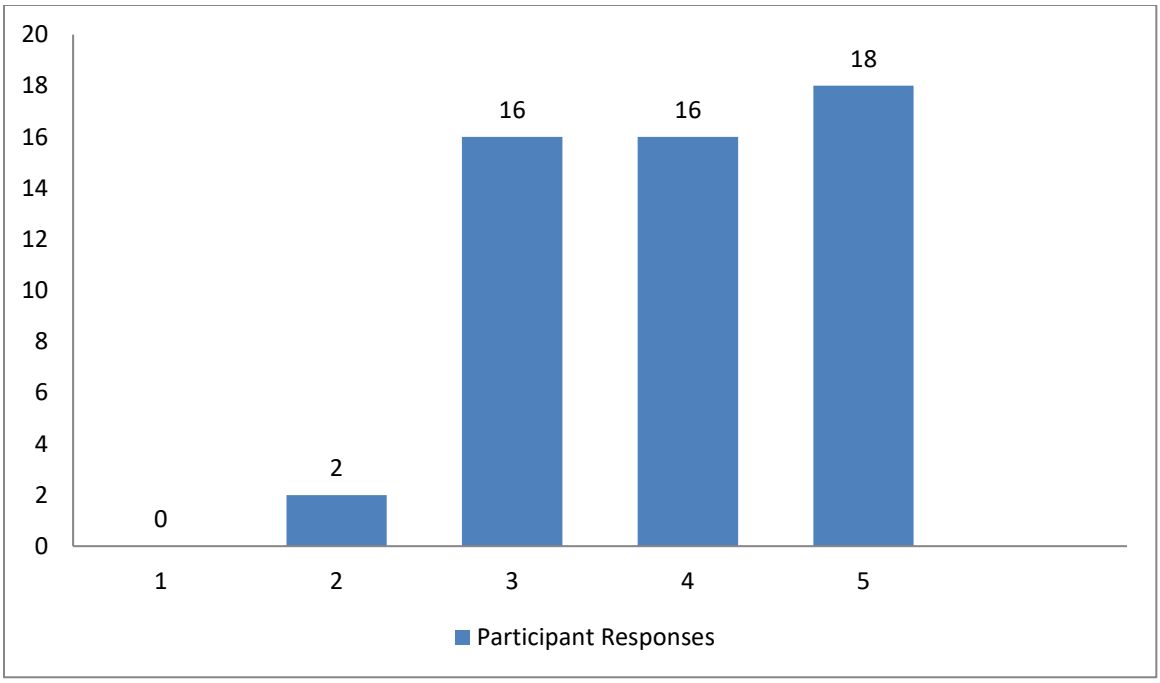
Source: NPS, 2021.

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



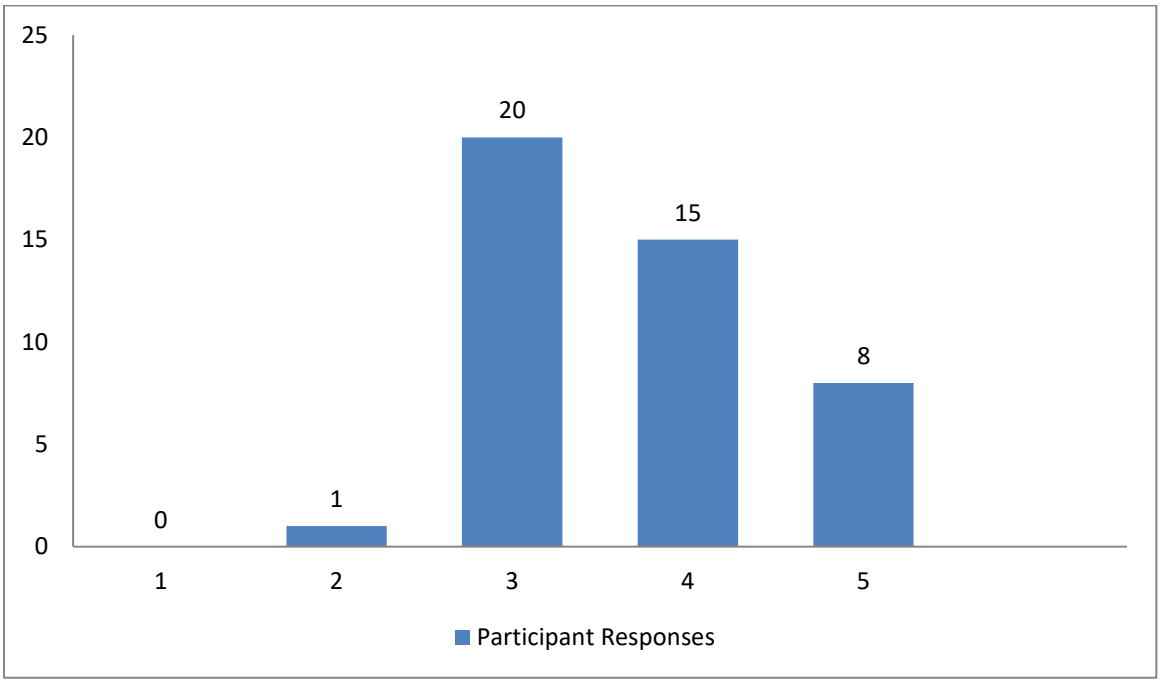
Source: NPS, 2021.

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



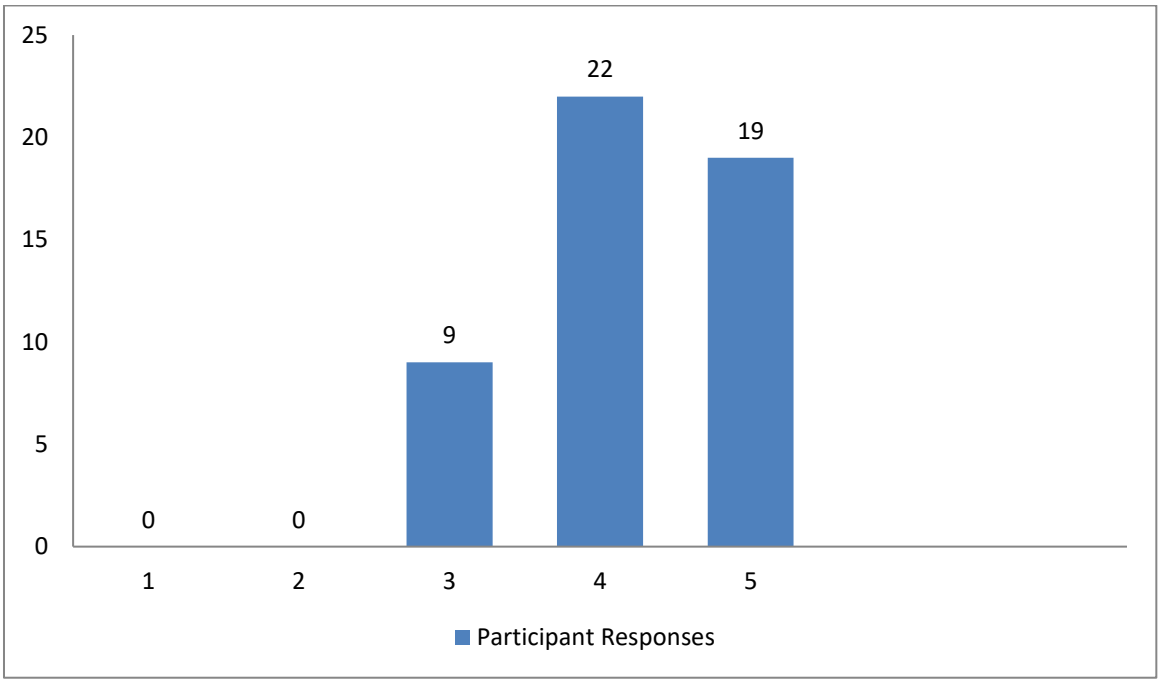
Source: NPS, 2021.

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



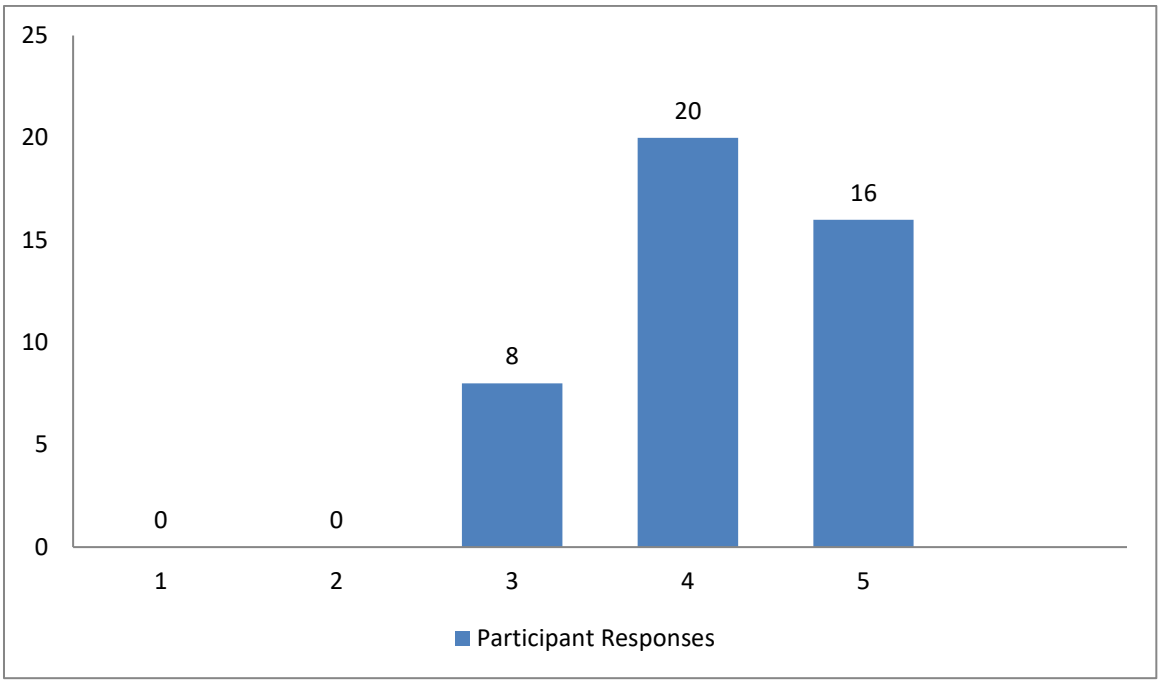
Source: NPS, 2021.

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, 2021.

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



Source: NPS, 2021.

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

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, or

- by electronic mail via: https://europa.eu/european-union/contact_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 at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications from EU Bookshop at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

KJ-NA-31020-EN-N

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub

ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

EU Science, Research and Innovation

EU Science Hub

Publications Office of the European Union

doi:10.2760/74397
ISBN 978-92-76-49466-9