Coherent Resilience 2024 Moldova Tabletop Exercise (CORE24-M)

12 – 14 March 2024

Chisinau, Moldova

Final Evaluation Report

Table of Contents

Abstract

Coherent Resilience 2024 – Moldova (CORE 24-M) was a Tabletop Exercise to enhance the resilience of the country's critical energy infrastructure against cyber and hybrid threats.
The Tabletop Exercise took place on 12-14 March 2024 in Chișinău, Moldova. The aim of the exercise was to support the preparedness of Moldova to identify, prevent and respond to hybrid (kinetic, sabotage, cyber) risks to Moldova's critical infrastructure and energy supply, with an emphasis on the nexus between cyber and energy security, and to provide actionable recommendations for enhancing resilience and improving crisis management. A spectrum of threats was introduced in the exercise scenario ranging from natural disasters to hybrid attacks and terrorism activities. CORE-24 M focused on deepening collaboration between Moldovan energy operators and cyber defenders, ensuring the country is prepared to deal with non-conventional security threats. CORE 24-M was a three-day national, interagency, and public-private sector event that was executed with an academic seminar, a two-day exercise, and an after-action briefings. This report focuses largely on syndicate responses to the exercise scenario and injects to include capturing key takeaways and recommendations. The event brought together over 100 participants from 10 nations and 32 institutions.

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 and NATO experts who led syndicate discussions:

Syndicate 1 - Critical Energy Infrastructure Protection - Cyber:
European Commission Joint Research Centre and New Strategy Center

Syndicate 2 - Crisis Management:
European Commission Joint Research Centre, NATO CMDR COE and NATO Civil experts

Syndicate 3 - Strategic Communications:
Lithuanian Armed Forces, NATO Civil experts and New Strategy Center

The core planning team, consisting of experts from NATO ENSEC COE, NATO HQ IHC, and ME RM, led the development of the exercise scenario and injects. Their efforts are greatly acknowledged.

The exercise lecturers, consisting of experts from EC JRC, NATO HQ IHC, NATO CMDR COE, the Lithuanian Armed Forces, and US NPS, are greatly acknowledged for their knowledge sharing and interactions.

Excellent contributions from the TTX Evaluation group, including members from US NPS, NATO ENSEC COE, and NATO CMDR COE, in collecting information for this report are greatly acknowledged.

Victor Parlicov, Moldova's Minister of Energy, delivering opening remarks

1. Introduction

1.1. Coherent Resilience Program

CORE24–M held in Chișinău, Moldova from 12 to 14 March 2024 was the inaugural national and regional level Tabletop exercise (TTX) executed by the NATO Energy Security Centre of Excellence (ENSEC COE) aimed at enhancing resilience of energy systems in an era of hybrid threats. Previously, CORE TTXs have been conducted in Ukraine (in 2017 and 2021), France (2022), Georgia (2022), as well as several national and regional level programs in the Baltic States since 2014.

1.2. Coherent Resilience Moldova Tabletop Exercise (CORE24-M TTX)

1.2.1. Overview

The CORE24–M TTX was planned with the goal of furthering Moldova's resilience against cyber and hybrid threats. TTX as well focused on Moldova's crisis response capabilities by enhancing inter-agency and civil-military coordination, planning, and preparedness.

The CORE24–M TTX was developed and executed by NATO HQ together with NATO ENSEC COE, US NPS and Ministry of Energy of Moldova.

1.2.2. Exercise Aim and Objectives

The aim of CORE24-M was to support Moldova's national authorities and energy sector organizations through academic seminars and a discussion-based exercise to assess and enhance the resilience of critical infrastructure and energy supply against hybrid threats and improve their crisis management capabilities.

The following objectives were identified for CORE24-M:

- Enhance Moldova's resilience against hybrid threats targeting energy infrastructure and ability to effectively detect, isolate, and mitigate the impact of cyber-incidents on Critical Energy Infrastructure (CEI).

- Support Moldovan Crisis Response authorities' capability to respond to situations caused by hybrid attacks on the energy sector.

- Exercise cooperation and coordination of strategic communications among Moldova's main energy and cyber sector stakeholders in order to effectively mitigate hostile propaganda and fake news; create proactive counter narratives related to the security of Moldovan energy sector.

1.2.3. Concept for the Event

The TTX was divided into three parts that included a series of presentations, syndicate work, and an after action "hotwash" session.

The first day of the TTX started with welcome remarks, followed by a series of expert presentations to better prepare participants for the TTX. Lectures included the following topics:

Critical Energy Infrastructure Challenges (European Commission Joint Research Centre), NATO's Role in Energy Security (NATO HQ) & Cyber Defence (NATO HQ), Crisis Management (NATO CMDR COE), and Strategic Communications (Lithuanian Armed Forces). The opening plenary concluded with presentations by the Core Planning Team (NATO ENSEC COE) of the rules of the TTX, the exercise scenario and starting conditions, as well as the plan for exercise evaluation (US NPS).

Participants attend plenary sessions on diverse topics related to critical energy challenges, strategic communications, and cyber security

Part Two of CORE-24 M was the execution of the practical part of the TTX, the syndicate work. Participants were assigned to one of three different syndicate groups: (1) Critical Energy Infrastructure Protection (CEIP) - Cyber, (2) Crisis Management, and (3) Strategic Communications (STRATCOM). Each syndicate had facilitators to lead discussions and a small cell of evaluators.

Part Three of CORE-24 M consisted of the TTX After Action (or "Hot Wash") and debriefs. During the debrief session, each syndicate presented their key takeaways, assessments and responses to selected injects, and highlighted overall outcomes regarding identified areas for improvement

and best practices. The day was wrapped up by concluding remarks from the State Secretary of Moldova, NATO ENSEC COE representatives, Exercise Evaluators, and partner organizations.

Opening Remarks from Exercise and NATO ENSECCOE Director, Colonel Darius Užkuraitis (LTU)

1.2.4. The Final Exercise Report

This report focuses largely on the syndicate responses to the scenario injects to include capturing key takeaways – areas of improvement, best practices, and recommendations. Follow-on chapters provide reports for each syndicate takeaways. The concluding chapter captures the broader key takeaways that are relevant beyond one syndicate.

The exercise was based on a fictional scenario that closely resembles regional realities, so syndicate responses are generally completed in line with the scenario, while many key takeaways

were provided without reference to the fictional scenario. While Syndicates approached capturing exercise results in similar fashion, albeit with some differences, the intent was to enable groups to highlight important points in a manner that best suited participants and translate properly.

As is always with the character of the CORE TTX program, the writing of this report was a team effort.

2. CORE24-M TTX Scenario

2.1. Background and Scenario

As part of the assessment of the preparedness of Moldova's electricity and gas sector for various emergencies caused by hybrid threats, a baseline scenario was created. This reviews the geopolitical, socio-economic, climate, electricity and gas infrastructure, cyber security, and information operations resilience situation in the country in order to identify vulnerabilities and opportunities and, based on these, develop possible future crisis scenarios (vignettes and injects); this includes developing such injects for discussion, which will help relevant organizations identify potential risks and mitigate them through joint coordinated efforts.

The time period for the future crisis scenarios (vignettes and injects) is selected to be from December 2024 to January 2025.

2.1. Injects

Three separate Syndicates were developed, and – essentially – each Syndicate each hold a discussion based on the same injects. The three Syndicates each had representatives from the various ministries, security organizations, and energy industry as necessary to facilitate their focus area. The Syndicates were: 1. Critical Energy Infrastructure Protection - Cyber, 2. Crisis Management, 3. Strategic Communications.

The timeline of the crisis evolution:
- the crisis starts on December 22, Year 2024;
- the crisis scenario continues for 1 month until January 23, Year 2025.

2.2. Structure of Injects

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.

3. Syndicate 1: Critical Energy Infrastructure Protection - Cyber

3.1. Key Takeaways

Areas for Improvement

Secure, Resilient, Critical Energy Infrastructure and Systems. These can depend more on organizational actions and the "tacit knowledge" accumulated by key persons than advanced equipment or systems. Studies of engineering communities in the US have shown that key knowledge can exist as a series of informed practices, oftentimes left "tacit" or unwritten. There is perhaps no better example of the centrality of tacit knowledge in Critical Energy Infrastructure (CEI) than the execution of regular "islanding tests" and Energy Resilience Readiness Exercises (ERRE), which have proven powerful in uncovering flaws in CEI systems and procedures, allowing for their mitigation. Valuable technical knowledge about a CEI and systems is gained through such exercises. After a major US military installation performed an outage exercise, one participant noted that it brought critical questions to the forefront around what it means to achieve real CEI protection and security through resilience. **Recommendation(s):** Plan and conduct ERRE Tabletop exercises to understand the technical and Institutional aspects of CEI at the municipal level. Employ model-based systems engineering (MBSE) practices toward the development of digital twins of CEI at the municipal level. Use digital twins to simulate CEI under hybrid threats and "islanding". Train CEI workforce and emergency operators of CEI systems on digital twins. Use digital twins to help support decisions in crisis situations (see Apollo 13 movie.)

Energy Infrastructure Damage Assessment, Repair Teams, and Contingency Contracting. Much of the discussion was high level in the CEIP-C syndicate and cyber focused. However, Inject 1 included that there was significant weather induced damage to substations and transmission infrastructure. There is also a need to address CEI Damage Assessment and Repair Team preparation and training as well as contingency contracting capability and capacity. Gaps in both the emergency energy supply as well as contingency contracting were identified as areas for improvement. This is an area of overlap with the Crisis Management syndicate. **Recommendation(s):** Assess the risk of key repair personnel shortages during a crisis and consider mitigation measures whether it is Train the Trainer Programs where civilian repair professionals train military engineers or explore Mil-Civ partnerships where corporations hire a percentage of military reservists who can be activated in times of such crisis. Also assess what existing contracts are in place and their relative capacity to mobilize quickly and execute repair and recovery related projects. Gradually improve the terms of the contract with each renewal to benefit Moldova. This approach would allow Moldova to negotiate better terms over time, ensuring more favourable conditions for energy supply.

Operational Technology Processes. CEIP-C syndicate's inject responses highlighted the need for collaboration and information sharing among SCADA operators, industry peers, government agencies, and cybersecurity experts to exchange threat intelligence and best practices for defending against malware attacks. Participate in industry-specific information sharing and analysis centres (ISACs) or other cybersecurity forums to stay informed about emerging threats and vulnerabilities affecting SCADA systems were processes and organizational improvements that could improve operational technology cyber responses in the scenarios. **Recommendation(s):** Provide comprehensive cybersecurity training and awareness programs to SCADA operators, engineers, and other personnel to educate them about the risks of malware attacks and the importance of following security best practices. Develop and maintain a comprehensive incident response plan specifically tailored to address malware attacks targeting SCADA systems. Define roles and responsibilities, establish communication protocols, and conduct regular drills and exercises to test the effectiveness of the incident response plan.

Tailoring of Critical Infrastructure & Cyber Topic Approach. The inclusion of both Critical Infrastructure & Cyber topics into the same Syndicate and the same Injects resulted in a challenging environment for deep dives on each topic. There was a great deal of implicit knowledge in the group on both topics, however the approach resulted in exhaustive coverage of all topics without the level of detail which would have challenged the group on specifics and details. Without stressing the group on details and documenting their approach there are less actionable takeaways. **Recommendation(s):** More detailed instruction to the facilitators would aid in challenging the group to stay on topic and perform systematic and detailed deep dives and gap identification.

Power Plant Control, Balancing, & Energy Generation. Throughout the injects, CEIP-C syndicate identified numerous areas for improvements in the resiliency of power plant operations. Injects highlighted the need to diversify energy generation and explore alternative heat plant mechanisms to enhance resilience and reduce vulnerability to disruptions. Key areas highlighted were control (the need for redundancy), balancing systems and agreements with international partners, and diversity in energy generation. **Recommendation(s):** Balance the potential loss of power generation from alternative sources to ensure a reliable energy supply. Consider alternative heat plant mechanisms to minimize reliance on vulnerable systems. Explore different fuel options and alternative heating mechanisms to sustain the required minimum temperature within the pipelines. This would help ensure stability and resilience in the event of unexpected changes in power supply from Kuchurgan or power loss. Duplicate the power plant control/monitoring centre in Moldova to increase trust and enable better monitoring of processes. This duplication would enhance transparency and aid in the collaboration with neighbouring countries to balance the power grid during supply disruptions.

Improved Coordination, Response, & Planning. CEIP-C syndicate's responses to multiple injects showed that advanced planning and resource allocation are crucial for effective coordination during crises. The first 24 hours are critical, and plans should be in place to act even without communication infrastructure. Cross-border infrastructure issues need to be addressed in laws and planning. Actions should emphasize the importance of effective communication, diplomatic engagement, and technical solutions to maintain energy security and stability in the region. **Recommendation(s):** Crisis cells established by country councils should serve as the starting point for coordinating response efforts. It is important to have a short and mid-term plan for response, considering realistic hardware injects. The response plan should involve understanding vulnerabilities, conducting risk management, and training end-users. Cybersecurity measures should be integrated into critical infrastructure planning.

Counter Mis/Disinformation Mitigation Plans & Procedures. CEIP-C syndicate's responses to multiple injects required the coordination of whole-of-government operations across the cyber, information, social medial, and other spaces to combat a complex series of mis/disinformation attacks. Responses were effective, however there are several additional areas for improvement that go beyond the inject responses described previously in this report. **Recommendation(s):** Provide comprehensive cybersecurity training and awareness programs to government employees to educate them about common cyber threats, phishing attacks, and social engineering tactics. Establish procedures for verifying the accuracy and authenticity of content published on government websites to prevent the dissemination of misinformation or disinformation. Implement fact-checking mechanisms and collaborate with reputable sources to ensure that information presented on government websites is credible and reliable. This support includes training, tools, and procedures, as well as establishing a single point of contact for incident assistance. Developing private-public partnerships and outsourcing services, implementing managed detection and response, and partnering with universities for training are recommended.

Counter Unmanned Aerial System (UAS) Policies & Capabilities. The CEIP-C syndicate identified major gaps in the UAS space and there were significant contributions from the group regarding recommendations on almost every element of this complex problem set. It is worth noting that only limited work in this space such as establishing no-fly zones around critical infrastructure to restrict drone access has been performed. They emphasize the need for a multi-layered approach to drone security, combining preventive and protective measures, as well as continuous evaluation and adaptation of strategies to mitigate risks effectively while noting that any effective solution in this space will require large amounts of resources, policy changes, and technology. **Recommendation(s):** Analyse drone usage and improve legislation on drone fly zones and operations to empower critical infrastructure to implement anti-drone measures. Implement mandatory ID registration for legal drone purchases to enhance accountability and traceability. Implement electronic countermeasures, such as jamming, to disrupt drone control signals and

prevent unauthorized access. Employ physical barriers like nets to capture drones and prevent them from causing damage. Explore the use of directed energy weapons for neutralizing drones, although the feasibility and practicality of this approach should be carefully evaluated. Consider training birds of prey, such as eagles, for drone interception, although this may have limited application. Utilize detection systems such as radar and cameras, as well as radio frequency identification, to track drones and identify potential threats. Develop robust internal security protocols to address drone threats effectively. Continuously assess drone threats and prioritize mitigation efforts based on the severity of the risk. Implement a combination of technical, legal, and operational measures for a holistic drone threat mitigation strategy.

Best Practices/Strengths

Multiple Scenarios and Classification. Multiple scenarios should be considered to ensure preparedness. A general classification of infrastructure is needed to minimize the human factor and provide a framework for restricting network access in case of malware. Classification should be related to types of risk. **Recommendation(s):** A holistic approach to scenario and classification of infrastructure should be undertaken in order to prepare response teams for diverse challenges and aid in the implementation of best practices to enhance the country's resilience. Plans should be tested in practice, and employees should participate in simulated incidents. Orthodox calendar considerations and holiday-related attacks should be taken into account during exercises.

Gas Supply. If there is no gas supply from Russia, explore the option of sourcing gas from Moldova or the European energy market. Diversify power sources to reduce reliance on a single supplier. Invest in energy storage facilities to ensure a stable power supply. **Recommendation(s):** Facilitate a contract with a Romanian nuclear plant to enhance energy security. Note that a memorandum has been signed to improve connectivity with Romanian pipelines and electricity systems: The Cabinet has approved a memorandum of understanding with the Romanian Government on the implementation of projects necessary for the interconnection of the natural gas and electricity networks in Moldova and Romania. In the natural gas sector, the document provides for specific measures to increase the natural gas transmission capacity and for possibility of extending the Iasi-Ungheni-Chisinau gas pipeline by building a transmission pipeline around Chisinau by the end of 2031, IPN reports. Read more https://www.ipn.md/en/cabinet-approves-moldovan-romanian-memorandum-of-cooperation-in-energy-sector-7966_1102554.html#ixzz8UM0lsb67

SCADA Systems and Planning. SCADA systems should be connected, and supplies should be purchased in advance. Investment in training, education, and ensuring procedures and processes are not fully in place is necessary. SCADA responses should mirror the gas supply preparations (above) to ensure that load balancing, bottlenecks, and international support is available for SCADA responses. **Recommendation(s):** Establishing international agreements for power grid restoration, energy balancing, and rapid cyber reaction teams is being considered. The viability

and importance of exploring alternative shareholders besides Gazprom and utilizing alternative communication channels like Starlink were suggested. Identifying bottlenecks and using load balancers, terminating unwanted connections, and establishing legislation on drones and no-fly zones are additional recommendations.

Port and Physical Security. Ensure the force is experienced, educated, and motivated to handle such threats. Enhance perimeter security to prevent unauthorized access. Be proactive by using threat intelligence and increasing prevention measures. Share intelligence with other nations to catch the process and collaborate on addressing the threat. **Recommendation(s):** Test port security procedures to handle situations like the threat scenario presented. Increase the capacity to detect and defeat threats through sensors and scanning for explosives. Conduct training exercises to improve coordination and enable a quick response. Have relevant information posted and perform regular exercises to contact required authorities such as Ministry of Internal Affairs, Special Prosecution Office (Procuratura cause speciale), and Centre for Combating Cyber Crimes (Centrul pentru combatere crimelor informatice) for further investigation and support.

Threat Intelligence and Supply Chain Security. The call centres should gather information about incoming customer calls and trends to quickly identify ongoing billing issues. Contacting the authorities responsible for prosecuting crimes and national protection, including the police and potentially INTERPOL, to identify the source of the attack should continue to be the standard procedure. It is crucial to identify the source of the attack and the path that allowed the adversary to access the system. Determine if the error lies in the central billing services, the bank, or the energy supply, as multiple points of error are possible. **Recommendation(s):** Implement controls to detect irregularities, such as large invoices, and investigate the cause of the error. Utilize threat intelligence to identify potential terrorist attacks and disrupt the supply chain.

Cyber Best Practices. Measures are in place to prevent insider threats, with a responsible person/department available 24/7/365. DDoS attacks occurred during elections and were successfully mitigated. Implementing web application firewalls (WAF), next-generation firewalls (IDS/IPS), and increasing bandwidth and redundancy with ISPs are currently implemented cybersecurity measures. **Recommendation(s):** Preparation for wiper ware attacks is important, including procedures to disconnect targeted sites, isolate affected machines, conduct incident response, investigate the wiper ware, and restore systems. Protection of backups is crucial. The private sector may have false assumptions about being risk-free and should not overlook the national-level problem. Collaboration between national response teams and outsourcing contracts can be beneficial. The existence of a Cyber Security Centre of experts should be considered. The government should provide continuous support to make the newly created Cybersecurity Agency operational.

3.2. NATO civilian expert's recommendations

Improve Civil-military Integration

Civil-military integration between energy system owners, operators, and security and defence ministries in Moldova is fragmented and inadequate. Moldova does not conduct energy resilience-focused exercises that would bring all relevant government and private sector stakeholders together**.** Further exacerbating this is the fact that elements of Moldova's critical energy infrastructure are in Ukrainian territory, an area over which Moldova has little to no control.

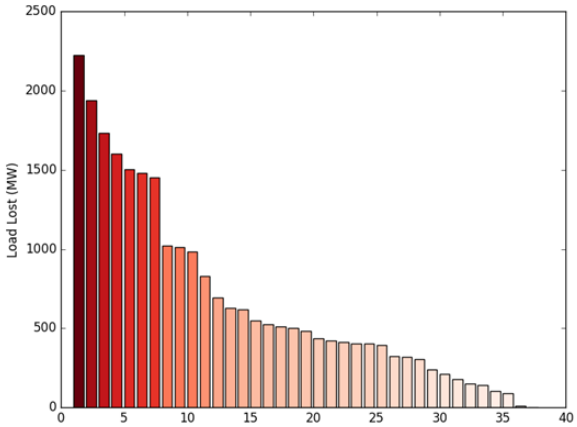
- Develop a robust civil-military integration planning and exercise program that will enable Moldova to anticipate, detect, respond to, and mitigate potential challenges before they become disruptive issues. Doing so will improve the security and resilience of both Moldova and its critical infrastructure partners.
- Ensure linkages between the civilian and military sectors in cyberspace, which are critical to facilitate crisis management and understanding of that grey zone scenarios involving cyber could be leveraged as part of hybrid threats against Moldova.

Identify and Protect High Consequence Failure Points in Energy Systems

Moldova depends heavily on energy imports to meet its energy consumption needs. In addition to receiving energy resources from neighbouring countries, Moldova also transfers a variety of energy resources to adjoining countries like Romania and Ukraine. These cross-border energy flows are not only critical to Moldova but, also, to the region**.**

- Conduct or utilize disruption modelling to identify high consequence failure points in Moldova's energy system. This modelling will enable Moldova's government, in conjunction with its critical infrastructure owners/operators, to identify and prioritize candidate infrastructure assets for civil-military protection and response planning.
- Assess high consequence failure points from the lens of physical security, including UAS, and cybersecurity.
- Furthermore, the assessments can identify potential mitigation measures like back-up generators or capital investments that improve security and resilience.
- These assessments will also help Moldova meet comprehensive EU accession conditions related to the defence of critical infrastructure, enhancing its partnership with NATO and integration into ENTSO-E.
- High consequence failure analysis example:
    - Protecting critical energy systems should focus on identifying potential failure points that would have the most severe consequences.
    - In this N-1 example, only 36 substations resulted in significant load loss and failures.

- This analysis can inform targeted planning and investment decisions (e.g., passive protection).

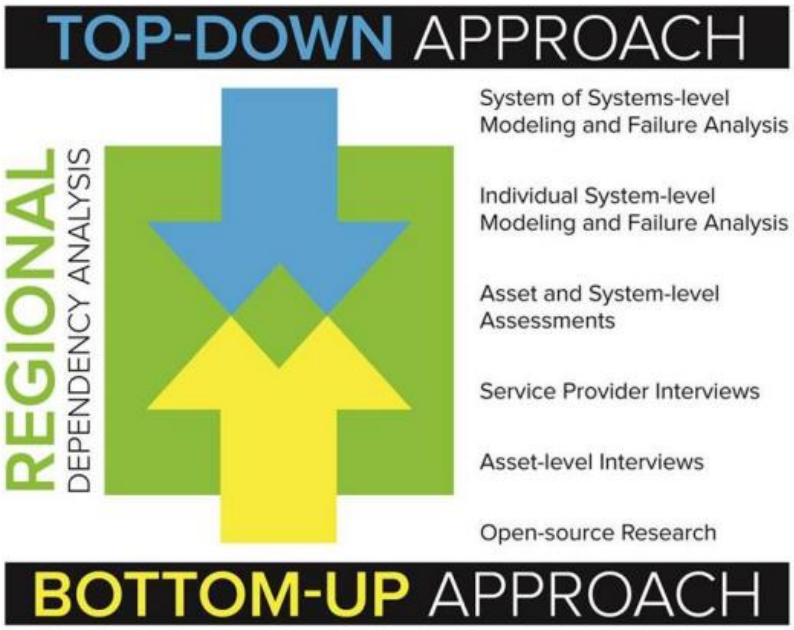


Source: Incorporating Prioritization in Critical Infrastructure Security and Resilience Programs - Homeland Security Affairs (hsaj.org)

Improve Coordination on Critical Infrastructure Protection

Moldova is exposed to multiple external and internal security threats, including from the war in Ukraine and of a cyber nature. Given these threats, the physical security and cybersecurity of Moldova's critical energy sites are inadequate. Physical security attributes such as access control, internal circulation, entry gates, and intrusion detection vary from facility to facility. Some of Moldova's critical energy sector assets have been modernized to include both information technology (IT) and operational technology (OT) systems such as supervisory data acquisition and control (SCADA). This exposes Moldova to emerging hybrid IT/OT/SCADA control environment threats.

- Leverage NATO, U.S., EU Partnership Mission Moldova (EUPM), or other technical assistance to design and implement a CIP program for Moldova and review existing national resilience models and legislation implemented by NATO allies. For example, Romania's CIP program includes an activity to "transfer expertise from Romania to increase Moldova's capacity to counter unconventional security risks, with a focus on CIP, cybersecurity, and hybrid threats.
- Improving the security and resilience of Moldova's critical infrastructure will support ongoing and future efforts to meet the European Union (EU) Critical Entities Resilience Directive (CER) and integration into the European energy system, particularly the ENTSO-E.



Source: [66506_f415finallewisandpetitcriticalinfra.pdf (unisdr.org)]

Remove Sensitive Information about Energy Infrastructure from the Internet

Sensitive information about critical energy infrastructure is publicly accessible on the World Wide Web, which adversaries can use to plan and execute nefarious actions that could induce significant disruptions to Moldova's critical infrastructure systems.

- Restrict the public release of sensitive critical infrastructure information to reduce the opportunity for adversarial disruptions to Moldova's critical energy infrastructure. Moldova should also explore language that modifies the existing transparency laws and makes exceptions for sensitive critical infrastructure information, which will also help avoid the potential for adversarial disruptions to Moldova's critical energy infrastructure.

4. Syndicate 2: Crisis Management

4.1. Key Takeaways

Areas of Concern

Counter Unmanned Aerial Systems (CUAS) Capability Gap. The current capability of UAS for detection and tracking should be upgraded. **Recommendation(s):** Reach out to countries that have or are currently dealing with UAS attacks and find out best practices. Identify low-cost solutions such as steel cable netting to add a layer of protection/hardening to critical infrastructure.

Non-Uniform Cyber Security Rollout. There is a lack of uniformity at the level of cyber security deployment across government institutions and the private energy sector. Cyber hygiene practices need further review and periodic inspection and testing. There may be overconfidence in the current cyber security levels, potentially leading to penetration. **Recommendation(s):** Hire white hat hackers for penetration testing. Zero trust philosophy should be embraced to begin securing against an attack at any level.

Best Practices/Strengths

Secondary/Emergency Dispatch Centres During Crisis. Some TSOs/DSOs already have secondary/emergency dispatch centres that activate should there be a compromise to the primary centre; however, not every TSO/DSO has this capability yet. During the COVID-19 pandemic, certain TSOs/DSOs employed a practice of social distancing by using multiple dispatch centres simultaneously. **Recommendation(s):** There is a new EU standard to abide by the required separation distance, so Moldova's compliance with the standard needs to be accelerated to all TSOs/DSOs. Cross-training between TSO/DSO dispatch operators may be useful for continuity of operations in a mass casualty event.

Distributed Power and Heat Generation, Diversity and Storage of Alternative Fuel Sources, and Potential for Microgrids and Medium Grids. Moldova is reviewing and discussing the concept of smaller co-generation plants that produce both electricity and district heating within the smaller regions and big cities. This allows dispersed power and heat production, therefore taking away the single point of failure from one large plant should it go down. Moldova already in some plants can switch between gas and coal (or other sources like oil or diesel). Moldova is also starting to review microgrids and medium grids to improve resilience. **Recommendation(s):** Smaller co-generation plants should be built and distributed around the country, which makes them harder to target. Plants should be multi-fuel capable (gas, coal, oil, diesel) and should have sufficient storage for back-up. Investment in microgrids and medium grids should move forward to improve

resilience. Using microgrids and medium grids, even if one portion of the country's power infrastructure goes offline, other portions can be powered and operate independently in a crisis.

4.2. NATO civilian expert's recommendations

Preliminary remarks on the crisis management recommendations: Crises can occur at any time and without warning and administrative management before or during a crises intervention can hardly be stopped in order to adjust the processes. Hence, changes must be brought about during ongoing operations in the sense of a learning system, the division into short, medium and long-term tasks is not suitable for crisis management. Since the developments are often ad hoc and unpredictable.
Rather, guidelines should be worked on continuously, which can also be used as a reference under operational conditions.

1. Change from centralized crisis management to holistic, decentralized crisis management
Smaller, autonomous units are more resilient than large units. At the same time, smaller autonomous units are easier to manage in crisis situations than large units. It has shown that one leadership entity can have the best overview over two to five units simultaneously. There is no need for a leadership entity below two to five units. It is important that each unit monitors its own situation and the state of the resources available to it.

2. Establish a mission rather than a control system
Systems that are driven by a mission or a common idea are more resilient to communication failures. They can act autonomously for a long time, but in the sense of the "Big Picture" (mission), if instructions are missing. Therefore, it is important to foster a common understanding of the goal, purpose and meaning of the operation as well as the valuable contribution of each staff member.

3. Separation between staff functions and experts in each critical area
Gathering and processing information, developing (alternative) plans, and preparing decisions are typical staff functions. In addition, critical infrastructure experts must be brought in to explain to decision-makers the impact of their decisions on the affected structure and the current situation. The more local knowledge they have, the more effective they will be. This is another argument for smaller regional crisis management units. Furthermore, previous experience in crises situation and/or training are beneficial for experts that may become relevant during a crises. A selection for trainings for experts must be made based on the results of risk analyses and the likeliness of scenarios while also bearing in mind not to cause public insecurity.

4. Early definition of responsibilities and roles and regular exercises

Responsibilities and roles must be defined in advance and their interaction must be regularly practiced. In order to maintain the flexibility of the actors, the use of different scenarios in such exercises must demonstrate that, despite these different approaches, certain tools and methods can be applied in a similar way. Exercises also enables the participants to act confidently when confronted with a real threats and practice helps to remain calm and focused.

5. Syndicate 3: Strategic Communications

5.1. Key Takeaways

Areas for Improvement

STRATCOM Plans (SOPs) at the National Level. STRATCOM syndicate highlighted that most of the state organizations have a trained cadre of communicators. In crises, individual entities can autonomously provide messaging based on their expertise/areas of responsibility. The lack of a single STRATCOM authority to assure proper interagency coordination during crises could impede effective message dissemination. Success hinges on identifying a single entity (or a designated group of representatives under a cell or committee at the national level) in charge to ensure coherent and well-coordinated information flow necessary to facilitate smooth coordination throughout the vertical and horizontal structures, based on mutually accepted and standardized processes. **Recommendation(s):** Uniform guidelines, formal plans and processes, and Standard Operating Procedures (SOPs) could be established to ensure the effective implementation of STRATCOM measures. Additionally, these documents should clearly outline objectives, key stakeholders and communications channels, messaging criteria, etc. Once SOPs are complete, it is important to train personnel on requirements to ensure stakeholders are in sync when it comes to the implementation steps.

Dependable Communication Tools during Crisis Situations. Participants underscored the importance of sharing information with people and organizations during crises. Prompt, reliable, and accurate communication practices during emergency situations are essential to ensure public safety, trust, and cooperation. The most utilized emergency communication tools include TV, radio, landlines, and the 112-emergency number. **Recommendation(s):** Aside from traditional means of communication, there is a growing need for introducing user-friendly communication tools to the Public. Stakeholders need to raise awareness about commonly reliable emergency communication tools (non-traditional and creative) ranging from low-tech to no-tech options, that could be utilized alternatively at times of blackouts or limited connectivity, speed, and reach. These could include leaflets, battery-generated radio station(s), public announcements, word of mouth, etc.

Tailored Messages for Affected Populations. There is a difference between levels of crisis impact among different strata. As such, crisis communication must adapt to their audiences considering the two separate municipalities affected and the difference in their transmission of messages. Narratives and messaging specific to the communities most affected by the crisis would be required compared to transmitting one standardized message. **Recommendation(s):** Emergency and crisis management stakeholders should be aware of means of communication suitable for different groups and customize their messaging accordingly. Effectively customizing messaging and narratives would involve following rigid criteria through established SOPs to effectively address vulnerability for specific populations, such as age (children and elderly), geographic risks, abilities, socio-economic impact, and more.

Wider Access to the Internet. Some pockets of the Moldovan population have limited access to online information. In a crisis, it is critical that everyone can access reliable information quickly and easily. According to the World Bank Data, digital penetration and usage in Moldova are estimated slightly above 70%. **Recommendation(s):** Stronger broadband infrastructure, affordable and equitable access, as well as the development of public-private partnerships (e.g. Starlink) would be instrumental in improving internet capabilities in remote areas, especially for vulnerable groups of the population. In areas where internet access is not feasible, alternative sources of communication need to be implemented.

Enhancing Emergency Plans and Training. Even though participants discussed plans that should be in place, the degree of shared awareness about the plans and training of personnel remained unclear. The need for each Ministry to identify and train emergency response personnel as well as establish internal emergency response plans was identified. **Recommendation(s):** The Inspector for Emergency Situations could lead the effort of synchronizing emergency response procedures, plans, and training of personnel to ensure effective and efficient crisis management across stakeholders. Local municipalities could also develop, maintain, and rehearse their own Emergency Response Plans in synchronization with the national-level plan(s).

Lead Entity to Ensure Cohesive STRATCOM. During the discussion, participants noted a few key entities that need to be involved to ensure effective STRATCOM processes. However, the involvement of multiple entities without a clear focal lead could cause overarching communication challenges. Upon further discussion, the syndicate agreed that the Government should lead the effort in close coordination with other ministries involved. **Recommendation(s):** There must be an institutional leader in this multilayer communication effort. Official interagency mechanisms need to be developed to formalize interagency cooperation. Once developed, lead ministry personnel would require training on the practical aspects of conducting such communications and liaison processes.

Cross-Sectorial Communications Mechanism. The syndicate emphasized that the Government should implement necessary measures to combat disinformation circulated by TASS through centralized message transmission, blocking sources that propagate false information, posting examples of previous disinformation on the official websites, equipping citizens with guidance and credible sources, etc. **Recommendation(s):** Implementing cross-sectoral communication strategies for countering disinformation and effective STRATCOM response is pivotal. This approach would help build institutional capacity across sectors and ensure stronger response and awareness.

International Cooperation. Participants highlighted the role of international relations and cooperation as an important communication strategy. Participants discussed strategies pertaining to STRATCOM and countering disinformation through corroboration with external partners (e.g. embassies of partner countries, counterpart ministries, etc.). Additionally, the involvement of the State Chancellery/ Reintegration Office was deemed necessary for promoting dialogues with external administrations. **Recommendation(s):** Continuing to enhance and leverage international support and collaboration will be instrumental in implementing more effective measures to counter disinformation by providing more coordinated responses, frameworks, and processes.

Assessing Emergency Policies and Procedures. The Syndicate acknowledged that applicable organizations must have plans in place. However, it was not clear how rigorous their operational and technical components were, whether they were rehearsed with stakeholders, and if there were any assessments conducted. Only a handful of attendees had experience participating in Tabletop exercises, and the group recognized the need to practice existing plans to identify strengths, weaknesses, and opportunities for improvement. **Recommendation(s):** Emergency plans and policies should be exercised frequently in order to enhance awareness and implement necessary revisions and updates, as well as personnel training and interagency exercises as required.

Enhancing International Support. The STRATCOM syndicate focused on national-level cooperation, however, did not discuss reaching out to international partners to aid in crisis. With the current conflict between Russia and Ukraine, there are many non-governmental organizations (NGOs) operating within the region that can coordinate emergency aid. NGOs often have capabilities and logistical support but lack coordination. International Governmental Organizations (IGOs) also offer resource and logistical support that can be surged in a crisis event. Given the risk to human life of losing heat during the winter months in Ukraine, NGOs and IGOs offer an additional resource beyond domestic strategic energy reserves. **Recommendation(s):** Identify an administration within the government to coordinate support with relevant IGOs and NGOs. Having an ongoing effort to continuously identify NGOs operating within the region will also pay dividends in the event of a crisis. Identify a single governmental body responsible for keeping track of relevant aid organizations and coordination of response from each.

Interagency Cooperation. During STRATCOM syndicate deliberations, the newly established Centre for Combatting Hybrid Warfare was identified as a crucial participant in countering misinformation during a crisis. There was a lack of discussion on what the current capabilities and manning were for the organization as it did not have a representative at the exercise. Without proper knowledge regarding the manning or capabilities decisions were being made in its absence. **Recommendation(s):** Ensure the Centre for Combatting Hybrid Warfare is identified as a participant for any future exercises. Before any future exercises share the lessons learned with the Centre to develop standard operating procedures in line with the current organizational structure. Gaps can then be identified to better coordinate between agencies or develop the capabilities of the Centre.

Identify Domestic Support Programs. Given the physical and financial impact of an energy crisis, domestic sources of support will be the most expedient method to get immediate support to the public. **Recommendation(s):** To avoid public unrest the public not only needs communication, but also sources of support identified. Disinformation often seeks to widen the void of existing/perceived grievances. It would be important to combat grievances especially in the Transnistrian region of the Republic of Moldova given the contested nature of the area with Russia.

Develop Emergency Response Plan. Given the lack of prior interagency coordination, the STRATCOM syndicate did not identify a unified emergency response plan. Drone strikes in neighbouring countries during conflict are predictable, yet there was no current plan to execute between the members of the STRATCOM syndicate. **Recommendation(s):** Conduct an annual emergency response plan exercise between Moldova agencies. During this exercise review performance objectives, and identify hazards/threats, while identifying personnel, equipment, and communications that need to occur during each contemplated event. Conduct assessments at the local level to determine capabilities and response times based on the potential location of threats to infrastructure. Lastly, identify gaps in capabilities and equipment that need to be filled through various measures including training and legislation.

Information Operations Planning. STRATCOM syndicate discussions focused on the importance of communication with the population but did not have standard operating procedures (SOPs) in place to guide discussions. Key players were often identified, however, there was a lack of a formal process to guide the discussion on the who, what, where, when, and why of each message. Given the significance of possible drone strikes, cyber-attacks, and possible gas shortages a formal process must be identified for each message. **Recommendation(s):** Develop an information operations template to guide discussions and effectively communicate between agencies what is being communicated. After the situation has been identified and agreed upon, the agency, target audience, tasks, purpose, and methods need to be identified. An established process will identify

gaps for organizations and possible opportunities for coordination to fill those gaps between organizations. National crises demand rapid communication and participation from citizens to avoid exacerbating conditions.

Identify Communications Plan Capabilities. STRATCOM syndicate discussions focused on crafting messages for communication plans but overlooked the practical limitations of different communication channels. **Recommendation(s):** While having pre-written messages for emergencies is crucial, their effectiveness depends entirely on how they are delivered. To address this, a national communications assessment of each delivery mechanism would be needed. This assessment would involve analysing how widely each method (e.g., internet, radio, TV) can spread information in different regions. By overlaying this data on a map, we can easily see which areas each method can effectively reach. We often assume the Internet is available everywhere, but it relies on physical infrastructure like cables or cell towers. Similarly, radio and television signals have limitations. Emergency planners need to be aware of these limitations to choose the most effective methods for reaching different areas. An assessment would also identify underserved portions of Moldova that may be targeted by disinformation based on a lack of access to communications from legitimate Moldova entities.

Unmanned Flight Systems Regulation. The STRATCOM syndicate briefly discussed the drone strike, however, given the strike occurred within the borders of Ukraine, only the response measures were contemplated versus preventative measures possible to mitigate the crisis. **Recommendation(s):** Establish national-level legislation regarding the operation of drones within the borders of Moldova. Without legislation, the vulnerability to drone strikes is increased based on the inability of local authorities to identify prohibited types or uses of drones. Develop a plan for the public to communicate any prohibited uses or sightings of drones within the borders of Moldova. While small drones may be operated by the public, drone swarms or medium to large drones are often tools used only by government or threat organizations. Ensure the public is primed to report sightings of drone swarms or larger drones utilizing the 112-system discussed during the exercise. Drone sightings may identify not only kinetic threats to infrastructure by threat organizations gathering intelligence on infrastructure vulnerabilities before a crisis event.

Disinformation Literacy Campaigns. STRATCOM syndicate members were confident citizens would be able to identify disinformation, however did not discuss any specific campaign on the part of the Moldova government. **Recommendation(s):** Inculcating citizenry to withstand disinformation is a constant process that requires constant coordination between governments and private companies. Campaigns should focus on education and awareness with recent examples from the region while building unity by providing citizens with a method to easily report disinformation to the correct government entity. Build partnerships with independent fact-checking organizations while encouraging media outlets to only report after a reasonable attempt at verifying the information has occurred.

Cybersecurity Investment Recommendation(s): The majority of cyber-attacks rely on some elements of social engineering. The most effective prevention is education and ensuring systems are regularly updated with the most up-to-date security patches. For the most critical infrastructure, best practices are to use login methods that utilize at least two or more authentication factors. The three authentication factors are something you know (passwords), something you have (Universal 2nd Factor keys such as YubiKey), and something you are (fingerprint or other biometric method). Identifying partnerships in the public and private sectors will also reduce the time needed to respond to cybersecurity attacks.

Best Practices/Strengths

Improved Emergency Response Services. The accession of Moldova into the European Union prompts developing and approving emergency and crisis response practices. One of the notable examples involves establishing dispatcher offices at the municipality level to enhance crisis management and response. The offices host specialized services of rescuers, firemen, and policemen, who are instrumental in ensuring effective and efficient responses in emergency and crisis situations. **Recommendation(s):** As Moldova progresses toward the path of EU membership**,** further implementation of best practices will help enhance the country's resilience.

Shared Understanding and Mitigation of Russia Dis-Information Campaigns. In the past several years, there have been many lessons learned from other neighbouring countries on how to mitigate and counter adversarial disinformation such as its successes in building population trust and countering disinformation. Participants highlighted that the public is being trained to depend on reliable sources of information and to identify fake information, especially in crises. **Recommendation(s):** Continue building shared awareness on the importance of enhancing information resilience, especially capturing lessons learned and best practices from neighbouring countries.

Enhanced Role of Emergency Management Personnel. Emergency management is a team effort and effective communication during any crisis is critical. In case of failure to spread the message via established communications channels, the Commission for Emergency Situations (at the local level) has to contact residents through people who are on site (police, firefighters, ambulances, etc.) to spread applicable messages to the public. **Recommendation(s):** This practice is a model for effective inter-agency crisis response and should be considered for partner nations that may lack such a robust system.

Message Consistency Across Multiple Channels. In crises, communicators must maintain and disseminate consistent messages in ways that would be compelling for various audiences to leave no room for misinterpretation. In the Republic of Moldova, it is a well-established practice for

institutions to take government messages *ad litteram* and further disseminate them across their channels of communication. **Recommendation(s):** Moldova's practice of consistent messaging is beneficial to other nations confronting similar challenges (those who have institutionalized top-down STRATCOM approaches).

Whole-of-Society Preparedness. During the syndicate discussion, the Finland example was brought up, which is based on the concept of comprehensive security, where the vital functions of society are jointly safeguarded by the authorities, businesses, civil society organizations, and citizens. To complement the example, the syndicate saw the assessment framework for countering disinformation, information influence, and foreign interference, as well as system-wide capabilities, developed by the NATO Strategic Communications Centre of Excellence. **Recommendation(s):** The illustrative framework discussed during the syndicate serves as best practice. Implementation of the framework tools would help strengthen readiness, response, deference, and national resilience.

Focus on Authority. Given the contested Transnistrian region of the Republic of Moldova, maintaining proper governmental authority during a crisis is imperative to ensure perceived grievances are not magnified by crisis or disinformation. **Recommendation(s):** Recent conflicts in the region have demonstrated the value of high-level leaders communicating directly with their constituents. Authorities can positively influence the public if the proper authority and personality are identified to deliver the message.

Social Proof and Unity. Social unrest will be amplified if a national identity does not continue to be built while illustrations of the public successfully following directions demonstrate the value of trusting instructions from the government of Moldova. **Recommendation(s):** Stakeholders need to continue tailoring messages through future STRATCOM discussions and plans around themes of unity and social proof.

Continue to Empower the Centre for Combatting Hybrid Threats. Disinformation continues to serve Russia both domestically and internationally. An effective counter strategy lies in leveraging lessons learned and best practices from regional stakeholders. **Recommendation(s):** Based on the proximity to Ukraine, Moldova must continue to leverage the Centre for Combatting Hybrid Threats to increase open government communication with the public, proactively identify false information, and regulate social media platforms for responsible content moderation. Knowledge of the Centre has been well communicated, however, their participation in future exercises would pay dividends.

Utilization of Lessons Learned and Recommendation(s): Continuing to learn best practices to build national-level resilience can be glossed from countries bordering Russia. Regulation of

unmanned systems demonstrates an opportunity to identify a vulnerability and utilize the public to identify drone sightings.

5.2. NATO civilian expert's recommendations

Short term

1. To communicate clearly. Formalise a crisis communications taskforce within either the offices of the Prime Minister or President with authority to lead the communication response in time of crisis, second communication experts from relevant departments and instruct, when appropriate, the Interior Ministry's General Directorate for Emergency Situations, and the Commission for Exceptional Situations. The taskforce should possess necessary resources to rapidly create a centrally managed and regularly updated 'script' describing the government's top lines that can be disseminated both vertically with government departments, and horizontally with emergency services and local municipalities.

2. To build on existing credibility. Publish coordinated, relevant, timely and tailored crisis messaging to the general public and specific affected audiences based on the government script. Messaging should focus on reducing the public's barriers to their essential needs (food, water, warmth, shelter) and be adjusted to meet the communications means available (e.g. leafleting, TETRA network, battery operated radio broadcast, loud speakers during national power outage). To demonstrate strong handling, present a recognisable government figure capable of delivering both difficult and positive messages following the Krebs format (what is known, not known, what the government is doing, what actions the public should take, when the next update is).

3. To encourage unity. Use Moldova's greatest asset, the Moldovan people. In times of crisis, the Moldovan public has demonstrated their ability to rally together and cooperate if given the right information and empowered to take action, such as during the Covid-19 pandemic and the acceptance of Ukrainian refugees in February 2022. Introduce simple behavioural science techniques to identify behaviours to avoid (i.e. those exposing citizens to harm) and encourage positive behaviours (i.e. resource sharing, civil volunteering and alerting others to credible information sources).

Medium term

4. To counter hybrid threats. Support the Centre of Strategic Communications and Combating Disinformation in establishing the necessary tools and resources to rapidly craft a whole-of-government narrative during crises. Strategic communications should focus on tackling the specific risk factors that enable disinformation/FIMI to cause harm (e.g. political issues,

identities), rather than reactively debunking individual stories. When appropriate, work with global partners, including the EU, US and UK to explain threats and attribute threat actors, including through declassifying intelligence.

5. To support civil resilience planning. Create a National Risk register of key risks, using findings from the NATO Core Resilience exercise and NATO Resilience Advisory Support Team (RAST) 2023 report to gauge risk likelihoods, impacts, potential solutions and assign specific departmental experts. The Risk Register can draw upon legislative authority provided by Government Decision on the Commission for Emergency Situations. To reduce duplicating work, audit existing plans across the Moldovan government to determine if individual crisis comms plans already exist and capture existing lessons learned.

6. Conclusion

CORE24-M was a national-level exercise aimed at enhancing the resilience of Moldova's critical infrastructure systems through high-level interagency participation. The engagement served as a critical platform for collaborating with more than 100 participants from eight countries and more than 30 organizations. The sequence of the presentations and syndicate work was both informative and instrumental in identifying critical infrastructure cyber security gaps, mitigation strategies, best practices, and recommendations applicable to the Government of Moldova.

The following key takeaways and recommendations – several of which were presented during the Distinguished Visitors Day/Hot Wash – are those identified by the broader syndicate teams that consisted of facilitators, participants, and evaluators who collaborated on the developed syndicate reports consolidated within the chapters of this report with topics that expand beyond specific syndicate focus areas captured below.

Syndicate of CORE24-M deliberating on one of the crisis injects

6.1. Concluding Exercise Key Takeaways and Recommendations

Areas for Improvement

Improved Coordination, Response, & Planning Across Government and Society. All syndicates identified that advanced planning and resource allocation are crucial for effective mitigation of crises. While some ministries and organizations have plans in place for certain crises others did not have plans or were unaware of the plans of the organizations they were going to coordinate with. Gaps existed in knowledge of what other organizations planned, capabilities in assessing damage done by a crisis, and little had been done to practice the plans that had been developed. Cross-border infrastructure issues need to be addressed in laws and planning. Agencies and organizations should emphasize the importance of effective communication, diplomatic engagement, and technical solutions to maintain energy security and stability in the region. **Recommendation(s):** Crisis cells established by country councils should serve as the starting point for coordinating response efforts. Response plans should involve understanding vulnerabilities, conducting risk management, and training end-users of the plan. Cybersecurity measures should be integrated into critical infrastructure planning. Assess the risk of key repair personnel shortages during a crisis and consider programs to develop a body of personnel for crisis situations, public and private. The Inspector for Emergency Situations could lead the effort of synchronizing emergency response procedures, plans, and training of personnel across

stakeholders. Emergency plans and policies should be exercised frequently with all stakeholders to enhance awareness and implement necessary revisions and updates. Reach out to international partners to leverage their support in providing for possible deficiencies in a crisis response or coordinating responses to shared crises.

Increased Cybersecurity Development. While the gas transmission lines currently operate without automated controls in Moldova, there are likely subsystems that are vulnerable to attack. Additionally, there is a lack of uniformity across government institutions and private energy companies on cyber security policies. This difference results in vulnerabilities that affect all or over confidence in some places that present a security risk. **Recommendation(s):** The most effective prevention is education and ensuring systems are regularly updated with the most up-to-date security patches. Implementing a zero-trust architecture as standard across all government, critical infrastructure facilities, and crisis response organizations. Identifying partnerships in the public and private sectors will also reduce the time needed to respond to cybersecurity attacks. Additionally conducting regular penetration tests to ensure networks are secured from possible malign intrusions.

Establish Counter Mis/Disinformation Mitigation Plans & Procedures. The syndicates' responses to multiple injects required the coordination of whole-of-government operations to combat a complex series of mis/disinformation attacks. Responses were effective, however there are several additional areas for improvement that go beyond the inject responses. **Recommendation(s):** Establish procedures for verifying the accuracy and authenticity of content published on government websites. Implement fact-checking mechanisms and collaborate with reputable sources through private-public partnerships and outsourcing services. Educating citizenry to withstand disinformation through coordination between government and private companies. Education campaigns should focus on awareness with recent examples from the region while building unity. Provide citizens with a method to easily report disinformation to the correct government agency. Build partnerships with independent fact-checking organizations while encouraging media outlets to only report after verifying the information.

Counter Unmanned Aerial System (UAS) Policies & Capabilities. All three syndicates identified major gaps in the UAS space and there was a variety contribution from each group on possible solutions. Only minimal work in this space such as establishing no-fly zones around critical infrastructure to restrict drone access has been performed. The groups emphasized the need for a multi-pronged approach to drone security developing preventive and protective measures, legislation, and a continuous evaluation and adaptation of each any effective solution in this space will require significant resources, policy changes, and technology. **Recommendation(s):** Analyse drone usage and improve legislation on drone fly zones and operations. Implement mandatory ID registration for legal drone purchases to enhance traceability. Implement electronic

countermeasures to disrupt unauthorized drone access to critical facilities. Employ physical barriers, i.e. nets or cables, at facilities to protect them against damage from attack drones. Utilize detection systems such as radar, cameras, radio frequency identification, to track and identify potential threats. Develop a reporting system where civilians can report unauthorized or suspicious drone activity and drone swarms to authorities. Finally, work with allies and partners to coordinate interception of UAS threats and develop cost effective interception techniques based on allied and partner experiences.

Best Practices/Strengths

Whole-of-Society Preparedness. During the syndicate discussion, the Finland example was brought up, which is based on the concept of comprehensive security, where the vital functions of society are jointly safeguarded by the authorities, businesses, civil society organizations, and citizens. To complement the example, the syndicate saw the assessment framework for countering disinformation, information influence, foreign interference, and system-wide capabilities, developed by the NATO Strategic Communications Centre of Excellence. **Recommendation(s):** The illustrative framework discussed during the syndicate serves as best practice. Implementation of the framework tools would help strengthen readiness, response, deference, and national resilience.

Multiple Scenarios and Classification. Multiple scenarios should be considered to ensure preparedness. A general classification of infrastructure to codify critical infrastructure and procedures relating to that codification. Classifications should be related to types of risk the infrastructure would be exposed to. **Recommendation(s):** A holistic approach to scenario and classification of infrastructure should be undertaken in order to prepare response teams for diverse challenges and aid in the implementation of best practices to enhance the country's resilience. Plans should be tested in practice, and employees should participate in simulated incidents.

National Single Service for Emergency Number. For emergency services (fire, police, ambulance) one emergency number is used, which is 112. The practice has evolved since Soviet times, when each of the services had separate numbers. The government of Moldova issued the decision to use one single number for emergency situations in 2016. The public has been trained in the processes, call taking, dispatching, etc., and advanced mobile locations are integrated through various technological means. **Recommendation(s):** This best practice can be implemented in countries that lack a national single service number for emergency situations to ensure efficient emergency response.

Utilization of Lessons Learned. Moldova learned from the experiences of neighbouring countries and extended energy supplies through national-level legislation. **Recommendation(s):** Continuing

to learn best practices to build national-level resilience can be gleaned from countries with similar security concerns.

6.2. Closing

It is important to note that this report – ideally – does not end CORE24-M, for Moldovan ministries and organizations that participated in the TTX should each develop an Improvement Plan based on the relevant key takeaways identified. Each institution is to further analyse 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 institute changes to further the efficiency and effectiveness of their organizations' responses to challenges related to critical energy infrastructure and hybrid threats – such a product would constitute their Improvement Plan. Further, the ENSEC COE has developed an initiative to 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 CORE24-M.

Remarks by Dr. Dan Nussbaum, TTX Evaluation Group Director, Energy Academic Group Chair, NPS.

Addendums

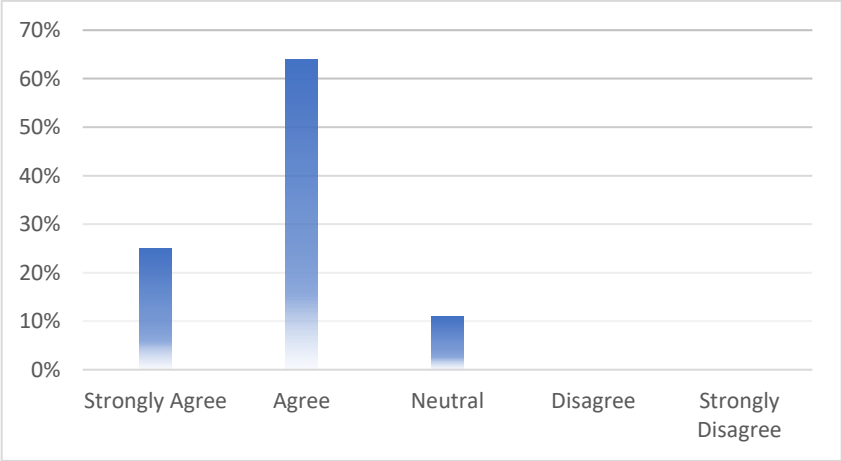
List of Participating Organizations

- NATO HQ, Innovation, Hybrid and Cyber Division
- NATO Energy Security Centre of Excellence
- NATO Crisis Management and Disaster Response Centre of Excellence
- US Naval Postgraduate School
- European Commission Joint Research Centre
- Strategic Communications Department of Lithuanian Armed Forces
- New Strategy Center, Bucharest, Romania
- Ministry of Energy of the Republic of Moldova
- Ministry of Foreign Affairs of the Republic of Moldova
- Ministry of Internal Affairs of the Republic of Moldova
- Ministry of Defence of the Republic of Moldova
- Ministry of Economic Development and Digitalization of the Republic of Moldova
- Ministry of Infrastructure and Regional Development of the Republic of Moldova
- Security and Intelligence Service of the Republic of Moldova
- General Inspectorate for Emergency Situations of the Republic of Moldova
- National Agency for Energy Regulation of the Republic of Moldova
- SE Moldelectrica (electricity TSO)
- JSC Vestmoldtransgaz (gas TSO)
- JSC Premier Energy Distribution (electricity DSO)
- SA RED-Nord (electricity DSO)
- JSC Chisinau-Gaz (gas DSO)
- JSC CET-Nord (CHP)
- JSC Termoelectrica (CHP)
- JSC ENERGOCOM (electricity and gas supplier)
- JSC FEE Nord (electricity supplier)
- OMV Petrom Moldova
- Moldova Energy Projects Implementation Unit
- Nodul Hidroenergetic
- Ministry of Energy of the Republic of Romania
- CONPET SA (ROU)
- S.N.G.N. Romgaz S.A. (ROU)
- European Union Partnership Mission in Moldova (Observer)

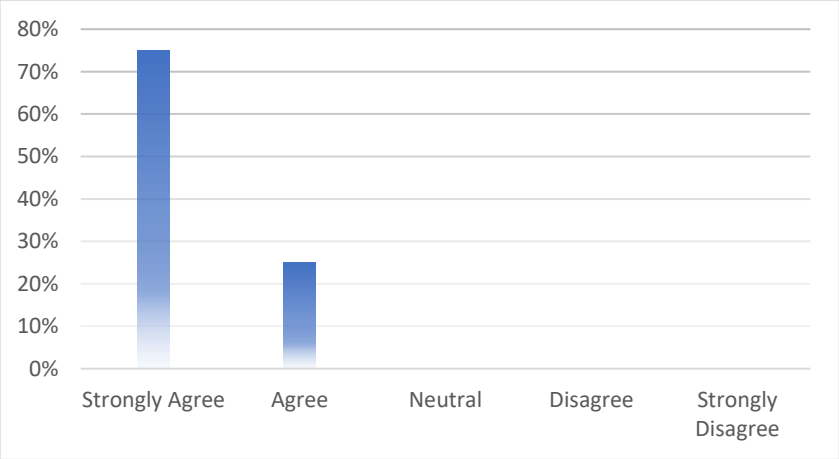
Results of Participant Exercise Evaluation Surveys

Quantitative Response Part I

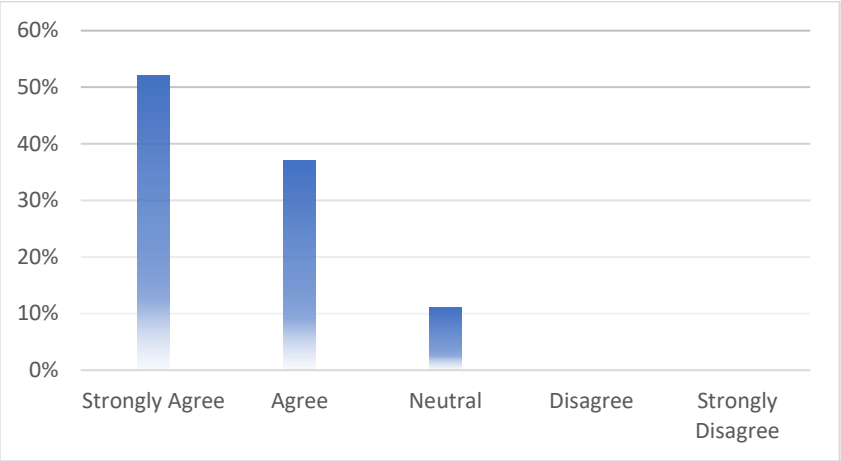
1. **TTX participants were present from the right organizations.**



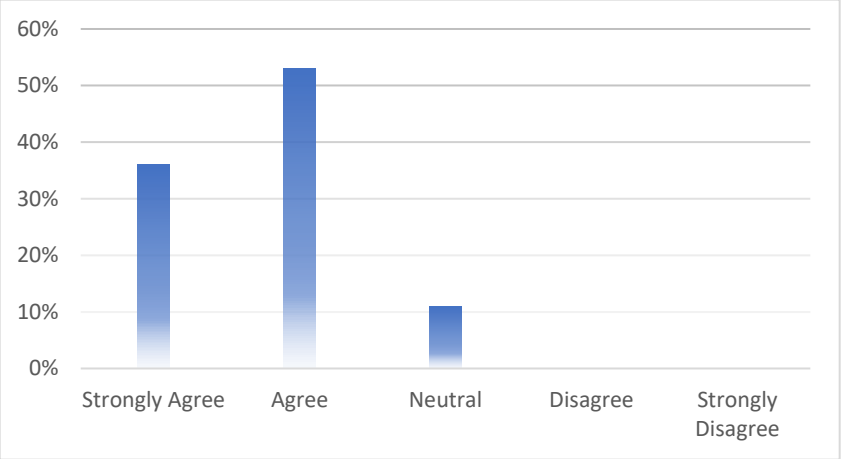
2. **There should be more educational opportunities (TTXs, seminars, workshops, etc.) in the future related to critical energy infrastructure resilience.**



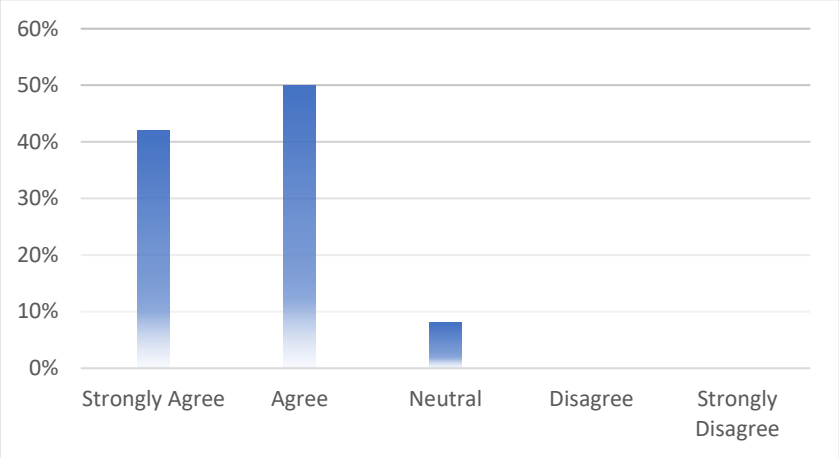
3. **My participation in the TTX was very beneficial to my current job.**



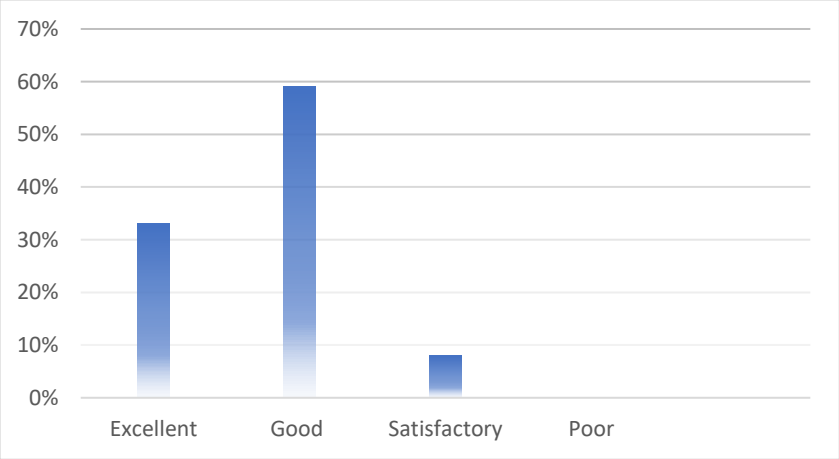
4. **Do you believe this engagement helped your organization to strengthen their capability to enhance emergency planning, prevention, and response to hybrid threats against Critical Energy Infrastructure?**



5. **After participating in this TTX, would you say your ability to support your organization/section in building resilience has increased?**



6. **How would you rate the strength of your organization with regard to collaborating with other organizations?**



Glossary of Acronyms

Acronym	Definition
AAR	After Action Review
CEI	Critical Energy Infrastructure
DSO	Distribution Systems Operator
ENTSO-E	European Network of Transmission System Operators for Electricity
EC JRC	European Commission Joint Research Centre
EU	European Union
GDP	Gross Domestic Product
HPP	Hydro Power Plant
ICS	Industrial Control Systems
IP	Improvement Plan
IS	Independent Study
IT	Information Technology
LNG	Liquefied Natural Gas
LPG	Liquefied Petroleum Gas
NATO	North Atlantic Treaty Organization
NATO HQ IHC	NATO HQ, Innovation, Hybrid and Cyber Division
NATO CMDR COE	NATO Crisis Management and Disaster Response Centre of Excellence
NATO ENSEC COE	NATO Energy Security Centre of Excellence
ME RM	Ministry of Energy of the Republic of Moldova

NPS	US Naval Postgraduate School
NSC	New Strategy Center, Bucharest, Romania
kV	Kilovolt(s)
GW	Gigawatt
OHL	Overhead Line
SCADA	Supervisory Control and Data Acquisition
SPP	Solar Power Plant
Toe	Tonne of Oil Equivalent
TPP	Thermal Power Plant
TSO	Transmission System Operator
TTX	Tabletop Exercise
TWh	Terawatt Hour
UGS	Underground Gas Storage
WPP	Wind Power Plant

Glossary of Terms

Term	Definition
Final Exercise Report	A Final Exercise Report (FER) is the final product of an exercise. The FER /Improvement Plan (FER/IP) has two components: a FER, which captures observations and recommendations based on the exercise objectives, and an Improvement Plan (IP), which identifies specific corrective actions, assigns them to responsible parties, and establishes targets for their completion
Capability	A means to accomplish one or more tasks under specific conditions to meet specific performance standards, and to achieve an intended outcome or objective
Critical Infrastructure	A set of infrastructure of the state that are the most important for the economy and industry, the functioning of the society and the security of the population, and the decommissioning or destruction of which may have an impact on national security and defense, the natural environment, lead to significant financial losses and human
Cyber Attack	Unauthorized actions carried out using information and communication technologies and aimed at violating the confidentiality, integrity and availability of information processed in the information and telecommunication system, or the violation of the sustainable functioning of such a system
Cyberspace	A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers that operate within and across these networks.
Sabotage	Commitment in order to weaken the state through explosions, arson, or other acts aimed at the mass destruction of people, causing bodily harm or other damage to their health, destruction or damage to objects of significant economic or defense importance, as well as actions specifically intended to cause radioactive contamination, mass poisoning, the spread of harmful substances, or other severe impacts on public safety and security.
Security of electricity supply	The ability of the electric power industry to provide the needs of consumers in electric energy in accordance with the requirements of Law
Data Collector	Exercise personnel selected from various agencies to evaluate and comment on designated functional areas of expertise; also referred to as an “Observer”

Term	Definition
Debrief	A forum for Planners, Facilitators and Evaluators to review and provide feedback in a facilitated discussion after the exercise is held
Exercise	A simulation activity held to train a single operation, command structure, or organization; provides opportunities to test plans and improve response proficiency in a risk-free environment
Exercise Timeline	Identifies the planning conferences and tasks necessary for planning and developing an exercise
Facilitated Discussion	The focused discussion of specific issues through a Facilitator with functional area or subject matter expertise.
Hot Wash	A facilitated discussion held immediately following an exercise among exercise Players from each functional area. It is designed to capture feedback about any issues, concerns, or proposed improvements Players may have about the exercise. Evaluators can also seek clarification on certain actions and what prompted Players to take them.
Improvement Plan	A grouping of one or more recommendations and action items identified to address weaknesses observed in an event; for each task, the IP lists the corrective action that will be taken, the responsible party or agency, and the expected completion date; included at the end of the FER
Moderated Discussion	A facilitated, discussion-based form where a representative from each functional area breakout presents to Participants a summary and results from a group's earlier facilitated discussion.
Observation	A recorded exercise activity
Evaluator	Exercise personnel selected from various agencies to evaluate and comment on designated functional areas of expertise; also referred to as a "Data Collector"
Out-brief	An assessment of areas in which an organization is doing very well, and areas which need improvement

Term	Definition
Object of the electric power industry	The electric power station (in addition to the nuclear part of the nuclear power plant), the electric substation, the electric network

Planning Team/Exercise Control Member	Any personnel performing a role or assignment as part of an Exercise Planning Team
Project Management	Coordination of personnel, resources, and strategic goals for a single exercise
Power plant	Electrical installation or a group of electrical installations intended for the production of electrical energy or combined production of electric and thermal energy
Real-World Event	An actual incident materializing threats to life, property, community, and the environment
Recommendation	The identification of areas for improvement observed during an exercise or experienced during a real-world event; based on root- cause analysis, recommendations are listed in all FER/IP's
Terrorist act	The use of weapons, the commission of an explosion, arson or other acts that created a danger to life or health of a person or causing significant property damage or other grave consequences if such actions were committed in order to violate public safety, intimidation the population, the provocation of a military conflict, international complication, or in order to influence decision-making or committing or not taking action by state authorities or local self- government bodies, officials of these bodies, legal persons, or attracting public attention to certain political, religious or other views of the perpetrator (terrorist), as well as the threat of committing these actions for the same
Vulnerability	A physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard


NPS
PRAESTANTIA PER SCIENTIAM
1909

GUVERNUL
REPUBLICII MOLDOVA

NATO ENERGY SECURITY
CENTRE OF EXCELLENCE

NATO
OTAN