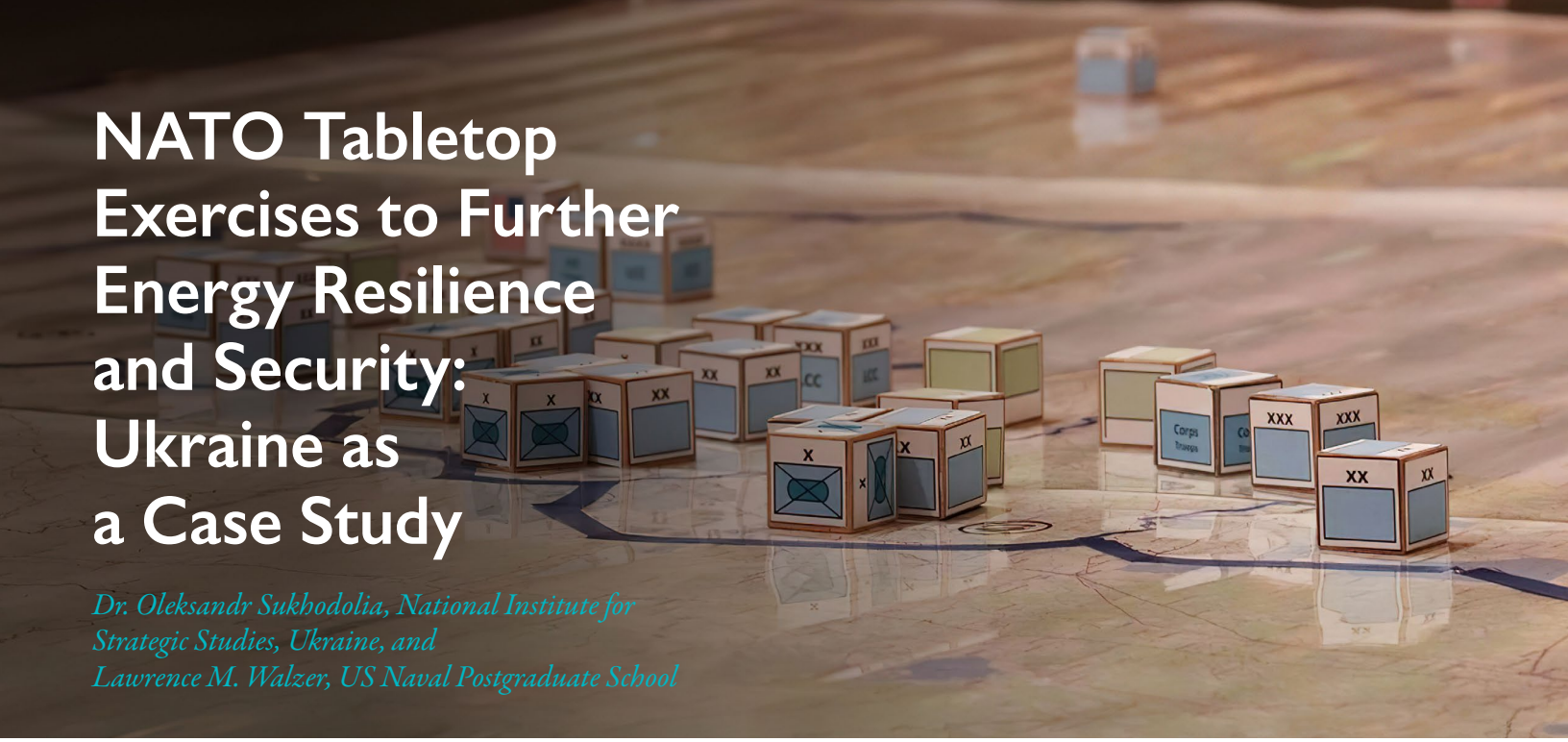

NATO Tabletop Exercises to Further Energy Resilience and Security: Ukraine as a Case Study

Dr. Oleksandr Sukhodolia, National Institute for Strategic Studies, Ukraine, and
Lawrence M. Walzer, US Naval Postgraduate School

FREEDOM, DEMOCRACY, AND SECURITY ARE threatened in many parts of the world by today's strategic competition and hybrid threats.[1]* Critical infrastructure (CI), including electricity grids, transportation systems, water systems, and so on, is an essential component of modern societies' economic strength, security, governance, and way of life. To mitigate the challenges posed by hybrid threats to CI, many nations are seeking to enhance the resilience of their critical infrastructure protection (CIP) systems through a range of legislation and government action. To assist with these endeavors, NATO and its associated Centers of Excellence have highlighted the tabletop exercise (TTX) as a tool to identify areas of concern and bring forth potential solutions, while the NATO Energy Security Center of Excellence (ENSEC COE) developed the Coherent Resilience (CORE) TTX program to focus on CI and hybrid threats. This paper looks at the design, development, execution, and outcomes of the CORE program, with special emphasis on the TTXs conducted in Ukraine in 2017 (CORE 17) and late 2021 (CORE 20).[2]

Various nations and institutions have their own definition of the term "tabletop exercise." The US Department of Commerce's National Institute of Standards and Technology guide on training and exercises defines tabletop exercises as "discussion-based events where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation."[3] This definition provides a useful understanding of the term as it is used in this paper.

The past several years have seen an increase in NATO exercises, many of which have also included partner countries. Thus, "following Russia's illegal 'annexation' of Crimea in March 2014, the number of exercises undertaken that year was increased and at their 2014 Summit in Wales, NATO leaders . . . have agreed on a strengthened deterrence and defence posture that draws upon all the tools at NATO's disposal, including military exercises."[4]

In Ukraine, a wider discussion of ways to adapt the national security system to hybrid threats resulted in the establishment of a program in December 2016 called the State System on CIP.[5] While developing the CIP system, government agencies identified significant shortfalls in interagency cooperation, as well as the absence of a common working language and procedures for communication.[6] A number of problems hamper the introduction of the CIP system in Ukraine,[7] but the following are the most important:

- the need to shift government and public attention from a *reactive* policy focused on recovering from the consequences of a crisis to *preventing* crises by developing the capability to deter, mitigate, and more effectively respond to hybrid threats;
- the need to establish a system of coordination among CI stakeholders, including effective public-private partnerships, that will enable them to combine their efforts; and

* This article was completed before the February 24 invasion of Ukraine by Russia, and so does not reflect that crisis.

- the need to clearly define the function of a CIP system in order to ensure the continuity of essential services and the resilience of not only CI but the CIP systems themselves during crises.

To make progress toward improving CIP systems, officials must first have full awareness of the problems. This knowledge would help ensure that the necessary legislation is put in place to coordinate planning in the institutions that are responsible for the various system components' activities, such as intelligence, counterterrorism, civil protection, cyber security, physical protection, and so forth. Increased awareness would also lead the population to better understand the challenges they would face in crisis situations and their role in supporting efforts to protect and increase CI resilience. The training programs usually associated with security and crisis management operations, however, often lack broad, interdisciplinary attention to CI and the continuity of essential services during crises. Among the various educational training tools that are available, collective exercises such as TTXs are the most useful for developing a common understanding among participating institutions, particularly those that are accustomed to working according to their own specific procedures.

> **The training programs usually associated with security and crisis management operations often lack broad, interdisciplinary attention to critical infrastructure (CI).**

The authors of this paper were directly involved in the design, development, and execution of a series of training events, in Ukraine and other Eastern Europe countries, that sought to highlight the objectives, structure, and challenges associated with conducting national-level TTXs on CIP.[8] Exercise design, development, and execution is a detailed and lengthy process, and covering every aspect of the exercise planning for these training events is beyond the scope of this paper. With that in mind, this paper will discuss the TTX as a training tool, focusing on the key aspects of exercise design and execution, and will conclude by describing some of the results from the CORE TTXs in Ukraine.

Tabletop Exercise as Training Tool

Many nations' military, government, and CI stakeholders are not familiar with tabletop exercises. Even NATO's Bi-SC Collective Training and Exercise Directive 075-003 (referred to as Directive 075-003 hereafter) makes no mention of them. It does, however, provide a sound planning process for exercise development, and serves as the primary source for NATO TTX planners, who will typically augment it with other NATO exercise directives, as well as doctrine from nations and organizations with detailed and formalized instructions related to TTXs.[9] The US Federal Emergency Management Agency, for example, has a well-developed TTX training program and online reference materials that proved to be very useful for increasing the preparedness of organizations, institutions, and nations for crisis events.[10]

In general, there are several types of collective exercises for planners to choose from, depending on the purpose. They are either discussion-based or operations-based, and each has specific purposes, goals, and outcomes.

Discussion-Based Exercises

- **Seminar**: generally focused on enhancing understanding and a common framework within a group, which can be a starting point for developing or changing plans, policies, and procedures; seminars often lead to a product such as a report.

- **Workshop**: organized to develop a product or, at a minimum, to collect and/or share information through discussions, lectures, and facilitated breakout groups.

- **Tabletop Exercise**: intended to generate discussion and can be used to enhance general awareness, validate plans and procedures, facilitate conceptual understanding, identify strengths and areas for improvement, and/or influence the perceptions of participants.

- **Game**: developed as an analog or virtual simulation of operations in which participants' decisions and actions enable them to explore decision-making processes and consequences and evaluate existing and potential strategies.

Operations-Based Exercises

- **Drill**: a coordinated and supervised event to validate a specific function or capability in a single agency/organization, often used to validate a single operation; goals include practicing and maintaining skills, preparing for future exercises, and potentially evaluating new procedures, policies, and/or equipment.

Members of the Strategic Communications Syndicate discuss exercise inject responses during NATO Coherent Resilience 20 held during the Black Sea TTX in Odesa, Ukraine.

- **Functional exercise**: a simulation in a real-time environment that is designed to assess the capabilities and functions of primary components such as command posts and staffs.

- **Full-scale (live) exercise**: a time- and resource-intensive exercise, usually conducted in a real-time, stressful environment, that is intended to mirror an actual incident; the goals are to demonstrate participants' roles and responsibilities and the ability of multiple agencies to coordinate their responses.[11]

A tabletop exercise was selected by NATO officials as the likely most effective method to facilitate Ukraine's efforts to develop greater CI resilience, given the current stage of its CIP system implementation. This is because the TTX is a low-risk, cost-effective tool that is designed to test and validate existing plans, policies, and procedures; highlight the capabilities of participating institutions; and identify resource requirements, capability gaps, strengths, areas for improvement, and potential best practices.[12]

TTX Design and Development

With the numerous resources available from national governments, organizations, agencies, and academic institutions, planners have a menu of options to support the design, development, and execution of TTXs. As mentioned earlier, the NATO planners who organized the CORE TTXs relied primarily on Directive 075-003, while also referring to other available sources as necessary and appropriate. The exercise design established a multi-stage event according to the three stages outlined in Directive 075-003: (1) exercise concept and specification development; (2) exercise planning and product development; and (3) operational conduct and analysis, and reporting. The next sections discuss a few key elements within each of these stages in order to provide a general overview of the critical aspects of planning and conducting a TTX.

Aim and Objectives

When designing an exercise, it is important to incorporate objectives that will achieve the overall goals that senior leaders intend the exercise to accomplish. In general, a TTX's objectives should be in line with an aspect of the exercise nation's and/or institution's past, current, and future planning activities.[13] If certain procedures are not yet defined in legislation or existing policies, the goal of the exercise may be to educate the participants about the specific challenges posed by certain threat or crisis scenarios, in order to identify any gaps that will require appropriate governmental or industry action to close. Objectives must be well-defined and achievable, and not leave participants feeling overwhelmed; such feelings can reduce active participation during the TTX.

In general, a TTX's objectives should be in line with an aspect of the exercise nation's and/or institution's past, current, and future planning activities.

The main purpose of CORE 17 was to involve Ukraine's government, industry, and nongovernmental organizations in meaningful discussions of how to respond to hybrid threats against critical infrastructure. The goal was to find gaps in existing crisis management plans, policies, and procedures, and to develop a consensus regarding what improvements needed to be made. Considering the status of Ukraine's CIP policy development and the exercise aims, these were the CORE 17 objectives:

- assess the resilience of CI and how well prepared the various system components were against hybrid threats (disinformation, cyber attacks, sabotage, covert operations);
- validate the effectiveness of national crisis management plans, policies, and procedures, including those that affect the energy supply, in their response to and ability to mitigate the effects and possible impacts of hostile hybrid actions;
- test existing measures to heighten the security of CI and supply chains, including those affecting military and civilian government institutions; and
- evaluate strategic communications procedures to mitigate the influence of malign hybrid actions, and to assess Ukraine's ability to coordinate with NATO members, partner nations, and international organizations.

These CORE TTX objectives reflected the needs of the different critical infrastructure sectors that ensure energy security and provide essential services.[14] Every relevant organization was involved in the planning process, precisely to ensure that all equities were considered in order to create a highly realistic, useful, and challenging exercise.

TTX Planning

For each CORE TTX, planners identified three stages for the weeklong event: a two-day academic seminar with presentations and discussions to orient participants; a three-day scenario-based TTX; and a one-day "hot-wash" (after-action discussion) combined with a Distinguished Visitors Day. The CORE 17 events took place as follows:

Academic Seminar (Monday-Tuesday): This stage included presentations and discussions on the topics relevant to the planned TTX scenario, to orient participants and make them aware of the latest information regarding types of threats, best practices, and any recent changes in legislation. This preliminary stage of the exercise was developed to ensure that participants had the information they needed ahead of time and were prepared for the actual exercise.

Participants of the CORE TTX at the National Institute for Strategic Studies in Kyiv, 17 October 2017.

Tabletop Exercise (Wednesday-Thursday): The exercise gave participants the opportunity to increase their understanding of issues associated with CI resilience as they responded to threats to the systems at both the national and local levels. The exercise also encouraged governmental and private entities to coordinate their responses to simulated threats.

After-Action Hot-Wash (Friday): Stage three consisted of after-action briefings and a Distinguished Visitors Day. The briefings summarized the results of participants' discussions on the scenario responses and highlighted best practices, areas for improvement, and recommendations. The Distinguished Visitors Day was attended by senior leaders from the host country and NATO countries to discuss the initial TTX results.

The Training Audience

The target participant audience for the Ukraine CORE TTXs included middle- and senior-level personnel from the following: government agencies and ministries in the fields of infrastructure (e.g., transport, energy), economy and trade (e.g., sectoral industries), emergency services, national security and defense (e.g., Army, police, intelligence), local authorities, and CI operators. The main task in selecting trainees is to include personnel who are responsible for CIP and national resilience at both the national and local government levels; members of relevant nongovernmental organizations and institutions; operators of critical infrastructure; and members of industry associations, the media, and so on. As with all exercises, it is imperative that participants be the right people, from the right organizations, and in the right number.[15]

> **The main task in selecting trainees is to include personnel who are responsible for CIP and national resilience at both the national and local government levels.**

Key Exercise Personnel

One of the most important factors of a successful exercise is skillful planning. Thus, the selection of key exercise personnel to fill the various roles in the TTX (exercise design, development, execution, and evaluation) is critical.

The following were some of the most important personnel roles for the CORE 17 TTX:

- **Exercise Planning/Control Team** developed and conducted the exercise, including the creation of a general plan for the training process, the exercise scenario, and all preparation materials and reference guides for facilitators and participants, and the coordination of training audience participation.

- **Participants/Players** responded to the exercise scenario based on their respective subject matter knowledge of current plans and procedures, and contributed insights to the discussions.

- **Observers/Subject Matter Experts** observed the exercise but did not participate in the discussions, except to provide answers to any technical questions that arose.

- **Co-Facilitators** were knowledgeable about and/or experienced in the subject material, and were responsible for keeping the discussions focused on exercise objectives. They also shared responsibilities for tracking time, announcing questions and injects (new events), following the discussion, and recording main findings and outcomes.

- **Evaluators/Data Collectors** gathered relevant information and ideas from the facilitated discussions during the exercise, so they could be incorporated into the final exercise report.

To ensure that everyone participates in the scenario-based discussions and that the allotted time is used most effectively, it is very important to have experienced and skilled facilitators. Some TTXs pair facilitators/moderators with assistant facilitators/moderators who play a secondary role, but we have found that having international experts and host-nation experts in co-equal roles is a better configuration for partner-nation exercises. At least one facilitator should be fluent in the host nation's language. Although they themselves do not participate directly in the discussions, facilitators must be able to both create an environment that encourages dialogue and guide discussions to prioritize key concerns and meet the objectives of the exercise. Because facilitators are often called upon to provide clarification on points of discussion, they need to understand the professional terminology related to the group's focus area, be experienced enough to make rational decisions, and be decisive enough to keep the discussion moving forward. Finally, facilitators must remain neutral and fair, and be comfortable with both allowing productive disagreements and ending fruitless debate if necessary.

Development of TTX Scenario and Exercise Events

Effective exercises are realistic and reflect current challenges confronting the exercise participants and organizations. For each CORE TTX, a Core Planning Team was designated and given responsibility for the development of the exercise scenario and corresponding events list—a series of vignettes and injects that are the basis for participant discussions.

The CORE 17 scenario was designed to reflect the kinds of real challenges to Ukrainian sovereignty posed by Russia in recent years.[16] It is clear that Russia developed a deliberate hybrid war plan for its 2014 operations in Crimea, designed to achieve limited but specific objectives. The early phase included a multi-faceted influence campaign that sought to discredit the government of Ukraine. This was done to shape the battlespace and help ensure the success of subsequent kinetic hybrid operations that ultimately led to the achievement of Russia's main objective: the forcible annexation of Crimea.

> **Russia explicitly attacked Ukraine's CI in all phases of its Crimea operations in order to exert psychological pressure on the population.**

Russia explicitly attacked Ukraine's CI in all phases of its Crimea operations in order to exert psychological pressure on the population and incite panic, social tension, and anger at the government; cause economic losses through the seizure of critical infrastructure and resources; and extensively weaken the government of Ukraine in the aftermath of the operation. It was in this context that CORE planners developed the TTX scenarios.

Each CORE TTX, all of which have focused on hybrid threats and energy security, has included significant elements of CIP. Using an "all-hazards" approach, the CORE 17 scenario and its injects comprised several different threats that would affect the continuity of services provided by CI.[17] The base scenario reflected lessons identified and learned from studies of Russian hybrid operations launched against Ukraine since 2014.[18]

Each CORE TTX scenario has consisted of four to five separate stages, such as (1) pre-conflict phase: hybrid influencing; (2) low-intensity hybrid operations; (3) conflict phase: high-intensity hybrid operations; (4) hybrid warfare; and (5) post-crisis stabilization. These stages reflect what planners view as most realistic based on the likely actions of the adversary and the necessity to "reset" after conflict subsides. CORE planning teams use the stages to identify sub-scenario vignettes and develop the corresponding event injects that will drive participant discussions. The vignettes describe the changing atmospherics that characterize each new stage in the exercise. A series of injects is then created for each vignette. For instance, an inject could be an explosion that takes place at a power generation facility and leaves the plant inoperable for several weeks. Participants would then discuss the likely effects of the power loss and the associated responses and obstacles. This is done for each inject that is presented.

To best accomplish the objectives of the CORE TTXs, participants are split into four or five "syndicates," each of which represents a different functional area. This format enables participants to focus their discussions on one specific area of concern according to the vignettes and injects.

Past syndicates have included:

- Strategic communications: focused on hostile propaganda and media manipulations as well as crisis communication;
- Site protection: related to cyber and terrorist attacks at the site, local, and national levels;
- Crisis response: concerned with energy-specific crises on the local and national level, and interagency interaction and information exchange; and
- International cooperation: working with allies, partners, international agencies, and nongovernmental organizations that may assist with crisis response and management at the international level.

The set of syndicates planned for each CORE TTX should reflect the exercise's objectives, so each TTX will likely have different syndicates. A brigade, for instance, could develop its own TTX with syndicates on command and control, operations, and logistics. Some exercises may not have any syndicates and instead keep all the participants in one group.[19] Such considerations also come into play during the development of injects: some injects may be relevant to all of the exercise's syndicates, while others can be targeted for specific syndicates. The general concept of injects and syndicate interactions during scenario-based discussions is shown in figure 1. In a typical TTX, the entire training audience begins in a plenary session, where facilitators present a vignette and lead an interactive discussion about it among the audience members. The syndicates then move to separate work areas, where facilitators present injects

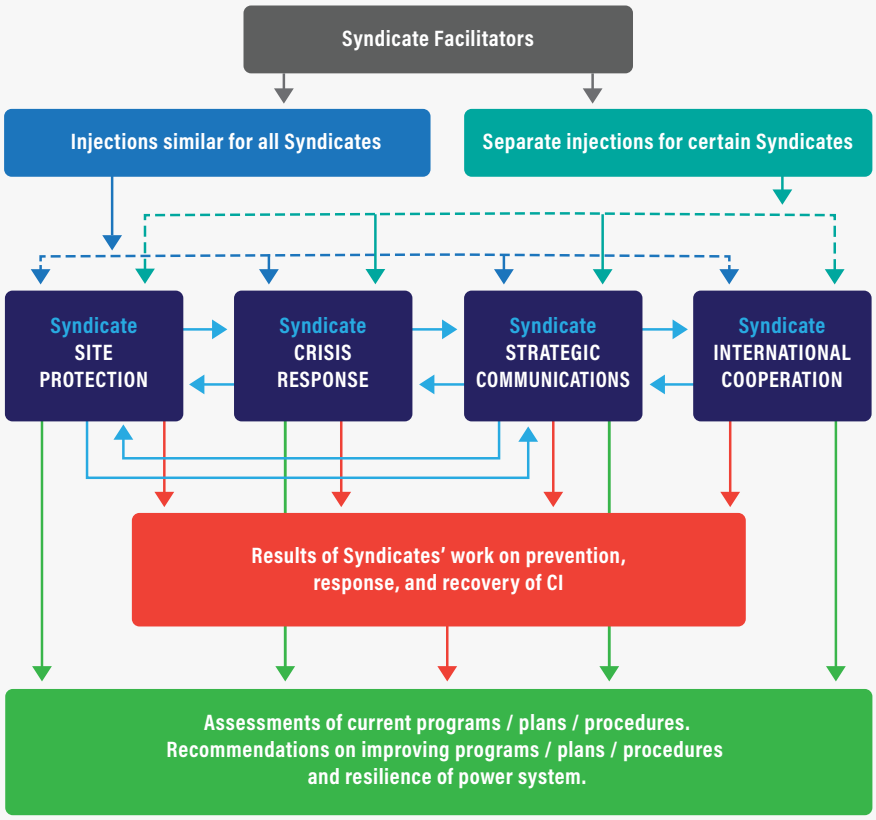

Figure 1: The General Concept of Injects and Syndicate Interactions[20]

for the participants to consider. Each syndicate can choose how to prioritize and spend time on the different injects it is presented with, but all of the syndicates must complete their discussions concerning that particular vignette within an allotted amount of time. Once the time expires, the training audience regroups for the presentation of the next vignette, and so on.

During the "hot wash" debriefing on the last day, each syndicate presents its work so that the rest of the audience participants can interact and discuss the key takeaways. In more recent CORE TTXs, efforts have been made to increase syndicate interaction with tools such as chat rooms.

Conduct of a Discussion-Based TTX

The vignette-based discussion is the main aspect of a TTX, so it is imperative that these discussions be focused and guided to meet exercise objectives. Both facilitators and participants need to understand what the discussions are intended to accomplish and how they will take place. Therefore, facilitators may require some training before the exercise, as well as access to detailed preparation materials and tools.

As described above, the scenario, vignettes, and injects prepared for a TTX are designed to stimulate discussion and encourage participants to do the following things:

- analyze the vulnerabilities of their critical infrastructure, determine the consequences of a system failure, an attack, and/or damage to CI, and evaluate the possible consequences for other related dimensions of society;
- assess whether and how well the institutions, agencies, and organizations that provide crisis response and continuity of services cooperate and coordinate their work;
- exercise both civil and military crisis management processes and civil emergency planning in response to aggressive hybrid tactics at various phases of a developing crisis; and
- determine the gaps in plans and procedures and outline possible legislative improvements.

The CORE 17 TTX syndicates discussed their scenarios in three parts. First was a conversation surrounding the detection of an incident; second was the response portion of the discussion; and third, participants talked about the policy aspects based on areas identified for improvement. Each discussion followed a series of predetermined questions:

Discussion of detection: How does this case qualify as a security incident? What current mechanisms are in place to detect threats? How is the information verified? Who should be informed immediately? Who activates the procedures for responding to a security incident, and under what conditions? How might the identified threats affect CI? Which critical services or functions would be endangered in the case of a crisis? What might be the immediate and long-term consequences of damage to these aspects of CI?

Discussion of response: What could be done to mitigate or prevent negative consequences? What role, tasks, and areas of responsibility does each of the involved departments, agencies, or organizations have during the response? Again, who activates the procedures for responding to a security incident, and under what conditions? How does interaction between CI operators and local and national government bodies take place? Are there procedures for ensuring continuity of the functions and services provided by CI if it is damaged? Are there mechanisms for preparing the population for action in a crisis? How will the state and industry leadership, mass media, population, and international partners be notified and kept informed of events?

Discussion of policy: Could this situation be prevented? Are there any mechanisms for preventing the crisis from escalating? What are the procedures for responding to an emergency situation and how are they regulated by law? Is there legislation in place to establish or revise the requirements for the protection of CI facilities and objects? What aspects of prevention and response need to be improved?

The TTX Final Report

The reporting phase of an exercise aims to provide a full analysis and evaluation of the exercise against its stated aims and objectives. This report captures events as they occurred during the exercise, provides an analysis of the events relative to the exercise objectives, and suggests follow-on development actions to enhance or improve participating agencies' planning and response capabilities. This is done through the development of key takeaways (areas for improvement, strengths, and best practices) from the exercise and corresponding recommendations.[21]

The CORE TTX series relies on teams of experts to conduct the post-exercise analysis and prepare a report. The US Naval Postgraduate School's (NPS) Energy Academic Group has provided an evaluation team that has worked together with the CORE planning team, facilitators, and participants to capture the results of each CORE TTX and develop the findings into a final report. To ensure the report's accuracy and relevance, it is often necessary to partner with a host nation entity that is familiar with the country's legislation, plans, policies, and procedures. In the case of CORE 17 in Ukraine, the host nation partner for the evaluation was the Ukraine National Institute for Strategic Studies (NISS).

The final report covers all aspects of the TTX, but its main value is the presentation of the results of the TTX and the key takeaways. The report also has a section for each syndicate that summarizes every vignette and inject that was included in that syndicate's discussions, and presents

Because high-level TTXs are not generally conducted on a regular basis, it is imperative that they are developed and executed in a manner that achieves the most comprehensive results possible.

Because high-level TTXs are not generally conducted on a regular basis, it is imperative that they are developed and executed in a manner that achieves the most comprehensive results possible. A detailed facilitators' guide, which is developed by the planning team and provided to facilitators ahead of the exercise, describes the exercise's goal, objectives, scenarios, vignettes, injects, and participating organizations. It also includes a series of discussion questions for the whole group and specific ones for individual syndicates or injects.

The TTX is not yet complete at the conclusion of the scenario-based discussions, of course. Now it moves to an analysis and reporting stage, which leads to the creation of a final exercise report.

the syndicate's key takeaways. The conclusion features a section of overarching findings that are common to more than one syndicate's discussions and/or apply to broader areas of CIP than a specific syndicate's area of expertise. Interagency communications, for example, often show up in final reports as a challenge across syndicates.

The team approach to developing the final report leverages all the knowledge and experience of the professionals who take part in the exercise. For instance, the NISS personnel were experts on Ukrainian legislation; the facilitators were subject matter experts from several NATO nations with expertise on NATO best practices; and the NPS evaluation group incorporated US best practices where applicable. Finally, the training participants included senior

professionals with years of experience in hybrid threats and CIP, whose ideas to improve energy security systems and resilience are invaluable and need to be captured.

Conclusion

The CORE TTX has proven to be an effective tool to engage various state and civil institutions in the evaluation and assessment of existing capacities to meet modern CIP challenges. These exercises are also a useful way to increase government and industry leadership's awareness of the importance of contingency planning. TTXs help to build interagency networking, create trust among government institutions and other key stakeholders, and establish a common language that enables every actor to understand the threats to CI and the obstacles to resolving them.

> **These exercises are a useful way to increase government and industry leadership's awareness of the importance of contingency planning.**

The CORE 17 and 20 exercises (conducted in 2017 and 2021, respectively) gave participants the opportunity to validate the policies, plans, procedures, processes, and capabilities that enable preparation, prevention, response, recovery, and continuity of operations in the event of a threat or disaster. The controlled environment of the exercises allowed the participants to safely explore real-world solutions that would both improve response communication and coordination and advance the efficacy of broad-based public-private CIP partnerships. In addition, the CORE TTXs produced a range of practical recommendations aimed at improving Ukrainian state policy on CIP and crisis management plans.[22]

Some of these recommendations have already been implemented through legislation. Soon after CORE 17, the Ukrainian government approved a resolution titled "The Concept for Building a State Critical Infrastructure Protection System in Ukraine," which outlines priorities for establishing a national CIP system and determines the main directions, mechanisms, and terms for the comprehensive legislative regulation of CIP activities.[23] The CORE 20 TTX was followed by President Volodymyr Zelenskyy's signature on a new law, "On Critical Infrastructure Protection," which serves as a roadmap to enhance the security architecture for CIP.[24]

The Ukraine CORE TTXs included a broad list of participants from NATO allies, partner countries, and international agencies that participated in the International Response syndicates. The goal was to review and assess the available means for international cooperation during crisis situations in a non-NATO country. Better coordination and cooperation between Ukraine and the international community in confronting Russia's aggressive hybrid operations have enhanced Western understanding of the adversary and deepened resolve to combat aggressive Russian activity throughout Europe and beyond.

Allies and partners seeking to improve national security and resilience against hybrid threats should consider implementing training and education programs that leverage TTXs as a means to identify areas for improvement, best practices, and potential solutions. There are several NATO entities that stand ready to provide assistance and expertise. Tabletop exercises, as demonstrated by the CORE program, are an invaluable means for allies and partners to further resilience and readiness to deter, deny, and defeat today's hybrid threats.

ABOUT THE AUTHORS

Dr. Oleksandr Sukhodolia is the head of Critical Infrastructure in the Energy Security and Technogenic Safety Department, Center for Security Studies, Ukrainian National Institute for Strategic Studies.

Lawrence M. Walzer is the deputy director of the Center for Combating Hybrid Threats, US Naval Postgraduate School.

NOTES

1. NATO identifies hybrid threats as combining "military and non-military as well as covert and overt means, including disinformation, cyber attacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace, and attempt to sow doubt in the minds of target populations. They aim to destabilise and undermine societies." "NATO's Response to Hybrid Threats: What are the Hybrid Threats NATO Faces?," NATO, 16 March 2021: https://www.nato.int/cps/en/natohq/topics_156338.htm
2. The CORE TTXs conducted in Ukraine in 2017 and 2021 were developed by the NATO ENSEC COE with the support of the NATO HQ Political Affairs and Security Policy Division (PASP), NATO HQ Emerging Security Challenges Division (ESC), and Cabinet Ministers of Ukraine. The NATO ENSEC COE has also executed CORE TTXs in the Baltic region and is in the process of planning two CORE TTXs in other regions.

3. Tim Grance, Tamara Nolan, Kristin Burke, Rich Dudley, Gregory White, and Travis Good, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, National Institute of Standards and Technology Special Publication 800–84 (Washington, DC: Department of Commerce, 2006), 4-4: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf
4. "NATO Exercises: Exercises Through Time," NATO, 1 February 2022: https://www.nato.int/cps/en/natohq/topics_49285.htm
5. Decree of President of Ukraine No. 8/2017, "On Improvement of Measures to Ensure Protection of Critical Infrastructure Components" [in Ukrainian], 18 January 2017: https://zakon.rada.gov.ua/laws/show/n0014525-16#Text
6. Oleksandr Sukhodolia, ed., *Developing the Critical Infrastructure Protection System in Ukraine* (Kyiv: National Institute for Strategic Studies, 2017): 81–83.
7. Oleksandr Sukhodolia, "Implementation of the Concept of Critical Infrastructure Protection in Ukraine: Achievements and Challenges," *Information & Security: An International Journal* 40, no. 2 (2018): 107-119: https://doi.org/10.11610/isij.4008
8. Oleksandr Sukhodolia, "Training as a Tool of Fostering CIP Concept Implementation: Results of a Table Top Exercise on Critical Energy Infrastructure Resilience," *Information & Security: An International Journal* 40, no. 2 (2018): 120-128:. https://infosec-journal.com/article/training-tool-fostering-cip-concept-implementation-results-table-top-exercise-critical
9. NATO, *Bi-SC Collective Training and Exercise Directive (CT&ED)*, NATO Bi-SC Directive 75-3 (Norfolk, VA: NATO Supreme Allied Commander, Transformation, 2013): https://www.act.nato.int/images/stories/structure/jft/bi-sc-75-3.pdf
10. "National Preparedness," Federal Emergency Management Agency, 21 December 2021: https://www.fema.gov/emergency-managers/national-preparedness
11. "Homeland Security Exercise and Evaluation Program (HSEEP)" (Washington, DC: Federal Emergency Management Agency, 2020), 2-6 – 2-11: https://www.fema.gov/sites/default/files/2020-04/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf
12. Ibid.
13. Natasha Rotstein, "Designing, Conducting, and Evaluating Tabletop Exercises: A Primer on Optimizing this Important Planning Tool," Center for Infectious Disease Research and Policy, 3 May 2007: https://www.cidrap.umn.edu/news-perspective/2007/05/designing-conducting-and-evaluating-tabletop-exercises-primer-optimizing
14. The CORE 17 exercise focused on critical energy infrastructure—specifically the national power grid—to facilitate contingency planning for the grid operator. CORE 20 focused on critical energy and transport infrastructure in the Black Sea region of Ukraine, with the goal to improve regional resilience against aggressive hybrid activity.
15. CORE 17 had more than 50 participants from Ukrainian ministries, agencies, and energy companies, in addition to 17 observers.
16. A vignette or scenario is "a sequential, narrative account of a hypothetical incident that provides the catalyst for the exercise and is intended to introduce situations that will inspire responses." Grance, et al., *Guide to Test, Training, and Exercise Programs*, D-2.
17. An all-hazards approach is an integrated approach to emergency preparedness planning that focuses on capacities and capabilities that are required to meet a full spectrum of emergencies or disasters, including internal emergencies, a man-made emergency, or a natural disaster.
18. Vytautas Butrimas, Jaroslav Hajek, Oleksandr Sukhodolia, Dmytro Bobro, and Sergii Karasov, "Hybrid Warfare Against Critical Energy Infrastructure: The Case of Ukraine" (Vilnius, Lithuania: NATO Energy Security Centre of Excellence, 2020): https://www.enseccoe.org/data/public/uploads/2020/11/hybrid-warfare-against-critical-energy-infrastructure-the-case-of-ukraine.pdf
19. In comparison with CORE 17, for example, the CORE 20 scenario introduced an additional syndicate, MARSEC, which dealt with maritime security problems and freedom of shipping, and separated cyber operations and kinetic attacks into different syndicates.
20. Figure 1 was created by the author, from Sukhodolia, "Implementation of the Concept of Critical Infrastructure Protection."
21. Vytis Kopustinskas, R. Šikas, L. Walzer, B. Vamanu, M. Masera, J. Vainio, and R. Petkevičius, *Tabletop Exercise: Coherent Resilience 2019 (CORE 19)*, EUR 29872 EN (Luxembourg: Publications Office of the European Union, 2019): https://enseccoe.org/data/public/uploads/2019/11/jrc118083_core_19_ttx_final_report_online.pdf
22. Sukhodolia, "Training as a Tool of Fostering CIP Concept Implementation."
23. "On Approval of the Concept for Building a State Critical Infrastructure Protection System," Resolution of the Cabinet of Ministers of Ukraine, No. 1009-r [In Ukrainian], 6 December 2017: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80
24. "On Critical Infrastructure Protection," Law of Ukraine No. 1882-IX (2021) [In Ukrainian], 16 November 2021: About critical infrastructure | from 16.11.2021 No 1882-IX (rada.gov.ua)