Information & Security: An International Journal

Sukhodolia, vol.40: 2, 2018, 120-128 https://doi.org/10.11610/isij.4109

TRAINING AS A TOOL OF FOSTERING CIP CONCEPT IMPLEMENTATION: RESULTS OF A TABLE TOP EXERCISE ON CRITICAL ENERGY INFRASTRUCTURE RESILIENCE

Oleksandr SUKHODOLIA

Abstract: Establishing a state-wide system of critical infrastructure protection requires significant efforts and investments. This is even more challenging for the countries that introduce this new approach into the everyday activity of the state agencies within existing state systems and procedures. The absence of a common working language, unified procedures of communication and interactions seriously hinders the process of establishing the critical infrastructure protection system in Ukraine. Training programs are believed to be useful tools contributing towards the purpose of building up proper foundation for further improvement of legislation and procedures in the field. One of the educational and training tools are the collective exercise, which are most relevant for developing common understanding of the problem by participants, who usually work separately. This article describes the Ukrainian efforts in providing personnel of the involved state agencies with knowledge of the policies, plans, methods and tools of critical infrastructure protection. The description of planning and results of the first national level table-top exercise on Critical Energy Infrastructure Protection "Coherent Resilience 2017" are presented in the paper as well.

Keywords: critical energy infrastructure protection, resilience, training, table-top exercise

Introduction

The importance of resilience of a national CI was recognized few decades ago and in last few years many countries developed a range of legislation that have helped them establish reliable state critical infrastructure protection (hereinafter – CIP) system. In Ukraine, wider discussion of ways to adapt national security system to modern threats was formalized through development by the National Institute for Strategic Studies (hereinafter – NISS) the Green Paper on Critical Infrastructure Protection [1] (October 2015) and later was recognized by the decision of the National Security and Defense Council of Ukraine which tasked the Government of Ukraine to establish the State System on CIP (December 2016).[2]

Working on implementation of the decision of the National Security and Defense Council, government agencies encountered a serious problem of interagency cooperation. The absence of working common language (terminology of different prevention, protection and response systems), unified procedures of communication and interactions (different systems work on their internal procedures) seriously hinders the process of establishing the CIP system in Ukraine.

In experts' view, a training program on CIP could help alleviate this problem. In addition, the training could provide potential students with knowledge of the policies, plans, methods and tools of CIP and to learn them to apply risk management techniques in enhancing security and resiliency of national critical infrastructures. One of the educational training tools is collective exercise, which is most relevant for developing common understanding of the problem by participants, who usually work mostly separately.

Table-Top Exercise as Training Tool

NISS, supporting the work of Government on the CIP Concept implementation, organized a series of workshops and seminars discussing the problem. These discussions resulted in raising public awareness of the importance of development of training programs in the area of CIP and brought the idea to organize a collective exercise aiming at building up common understanding and language between different state authorities in the field of CIP.

World best practice proposed set of exercises useful for this purpose:[3]

- Seminar, which generally orient participants to, or provide an overview of existing strategies, plans, policies, procedures, protocols, resources, concepts, and ideas;
- Workshop, which usually is employed to build specific products, such as a draft plan, policy, procedure;
- Table-top (discussion exercise), which is intended to generate discussion and can be used to enhance general awareness, validate plans and procedures, assess the types of systems needed to guide the prevention of, protection from, mitigation of, response to, and recovery from a defined incident as well as to facilitate conceptual understanding, identifying strengths and areas for improvement, and/or achieving changes in perceptions.
- Operations-Based Exercises (functional exercises), which are characterized by actual reaction to an exercise scenario and are used to validate functionality of plans, policies, and procedures; personnel performance and resource sufficiency.

- Full-scale (live) exercise is usually conducted in a real-time, stressful environment that is intended to mirror a real incident. Personnel and resources may be mobilized and deployed to the scene, where actions are performed as if a real incident had occurred.

In general, the choice of exercise is stipulated by cost effective way of achieving its aim and objectives. In case of Ukraine (in times of hybrid war against Ukraine and current stage of the initial CIP concept implementation) seminars and a table-top exercise were chosen as the most appropriate form of training of involved agencies personnel and checking consistency (availability) of current plans, standards, and procedures in the field.

Ukrainian lessons from a hybrid war of 2014–2016 years demonstrate the importance of critical infrastructure for national resilience, especially in regard to critical energy infrastructure (hereinafter – CEI). In this period Russia utilized different tools to undermine the ability of the energy sector to provide Ukraine with energy supply. Those have included damaging of CEI, blocking the supply of fuel for power plants, cyber and physical attacks, as well as use of propaganda to achieve synergy of the effort.[4]

Learned lessons from Ukrainian experience demonstrate that the damaging of critical infrastructure capability to perform its functions became one of the tools to diminish the country's ability to resist the aggressor. Malicious actions against critical infrastructure could become the tool of the state-aggressor, not just certain groups criminals (terrorist groups), as it was believed until now. In general, tensions between two or more countries or groups of countries can provoke attacks on energy supply system in order to destabilize society by undermining economic development and political will to withstand the deliberate aggression.

Thus, CEI comprising energy producing, transmitting and supplying elements is critical in terms of ensuring stability at political, economic and military levels and providing conditions for balanced development of a state. That is why it was suggested to organize first national level table-top exercise on the issue of resilience of critical energy infrastructure.

The idea of ь Table-Top Exercise on Critical Energy Infrastructure Protection (hereinafter – TTX) was jointly initiated by NISS and NATO's Energy Security Centre of Excellence as one of the practical steps in developing of earlier established partnership between institutions. TTX was supported by Ukrainian government and NATO that was reflected in Comprehensive Assistance Package for Ukraine, endorsed by the Heads of State and Government of the NATO-Ukraine Commission in Warsaw on 9 July 2016.

By this decision, Alliance countries provided support of Ukrainian efforts in building up national CIP system by means of sharing information and best practices in this field. NISS and NATO's Energy Security Centre developed a program of the event for wider involvement of participants not only from different Ukrainian agencies but also from NATO member countries.

The Concept of TTX

The table-top exercises named "Coherent Resilience 2017" (hereinafter – CORE 2017) pursued the following goals:

- to check existing procedures on prevention, protection and response on incidents related to energy sector; and
- to facilitate mutually cooperation departments in theirs action to provide resilience of the national power system, including international efforts to meet emerging security challenges.

Specific objective of the CORE 2017 was to identify the main aspects to be covered in developing an advanced Contingency plan for a CEI – United Energy System of Ukraine.

The target audience of the CORE 2017 was personnel of government agencies and ministries in the field of Energy, Emergency Services, National Security that included companies producing, transmitting and supplying electricity, government officials, military personnel, national police and other institutions and agencies responsible for protection and building resilience of electricity supply by improving plans, procedures and processes at a national level.

CORE 2017 was designed as multistage event that consisted of: Concept and Specification Development, Planning and Product Development, Operational Conduct and Analysis and Reporting.

At the Planning Stage there was developed a scenario with main focus on Resilience of United Energy System of Ukraine comprising generation, storing, transmission and distribution processes. The scenario was designed to comprise a number of threats under all-hazard approach that affect an uninterruptable energy supply. It includes natural disasters, technical malfunctions and cyber-attacks that are common in peace time as well as methods of hybrid warfare (sabotage, informational warfare, political destabilization, criminal activity) that was applied to Ukraine.

The scenario reflected threats to different elements of power system affecting production, transportation/distribution and supply of energy including fuel supply for generation capacities under different stages of potential conflict between two countries.

At the Operational Stage, CORE 2017 foresaw two stages: two days' Academic Seminar and three days' Scenario-based discussions.

The Academic Seminar provided presentations and discussions on four topics: the terrorist (kinetic) threats to CEI; the cyber security dimension of CEI; the management system in time of energy sector crisis; strategic communication in crisis.

The discussions on each of these topics were structured in delivering presentation on best available in NATO countries practice and learning Ukrainian lessons in countering hybrid warfare as well as question/answers sessions on following issues:

- threats identification, risk assessment and planning for security and safety incidents and crises involving critical infrastructures;
- response, emergency and contingency plans for critical infrastructure protection;
- learning Ukrainian lessons of countering attacks against critical energy infrastructure;
- role of personnel training and education in building resilience of CEI.

The scenario-based discussion was divided into four phases, namely: a) pre-conflict, b) conflict of low intensity; c) high intensity conflict and d) post-conflict situation.

The base scenario reflected the lessons learned by Ukraine from hybrid warfare launched against Ukraine (Sukhodolia, 2017). The following activities were identified as non-military means of warfare: (1) causing psychological pressure in order to spread panic, social tension and discontent with government; (2) causing economic losses due to seizures of CEI and energy resources, thus imposing additional economic burden on the country or getting additional resources for war; (3) obtaining local advantages by achieving a better position to pursue certain operations (combat collision, terms of contracts, ceasefire negotiation) or by forcing the government to do certain actions (payments, sale or purchase of resources); and (4) creation of a desired image in international community by making information campaigns in the mass media (cruelty of Ukraine in blocking energy and water supply).

Participants, divided in four syndicates, were expected to respond on vignettes and injections within existing in Ukraine response and emergency plans and procedures with focus on different aspects: STRATCOM Syndicate (dealing with hostile propaganda and manipulations as well as crisis communication), SITE PROTECTION (dealing with cyber and terrorist attacks at CEI site level), CRISIS RESPONSE (dealing with and energy crisis response on national level and interagency interaction and exchange of information), INTERCOOP (dealing with interaction and response at an international level).

Under scenario's injections participants were supposed to:

a) analyze vulnerabilities of critical energy infrastructure based on identified risks and threats,

b) determine the consequences of failure, attack and/or damage to critical energy infrastructure and impacts on other related dimensions of society,

c) determine cooperation and coordination between institutions, agencies and organizations establishing emergency services and assess their plans,

d) exercise crisis management processes, including military and civil emergency planning as a response to conditions provoked by hybrid means in pre-conflict, conflict and post-conflict situations.

The concept of the CORE 2017 Scenario gave the option for involvement of participants from NATO countries through direct participation in discussion by constituting separated syndicate INTERCOOP with the goal to check out available instruments of international cooperation in crisis situation in non-Alliance country.

The general concept of injection introduction and syndicate's interaction under scenario-based discussions is shown on Fig.1.

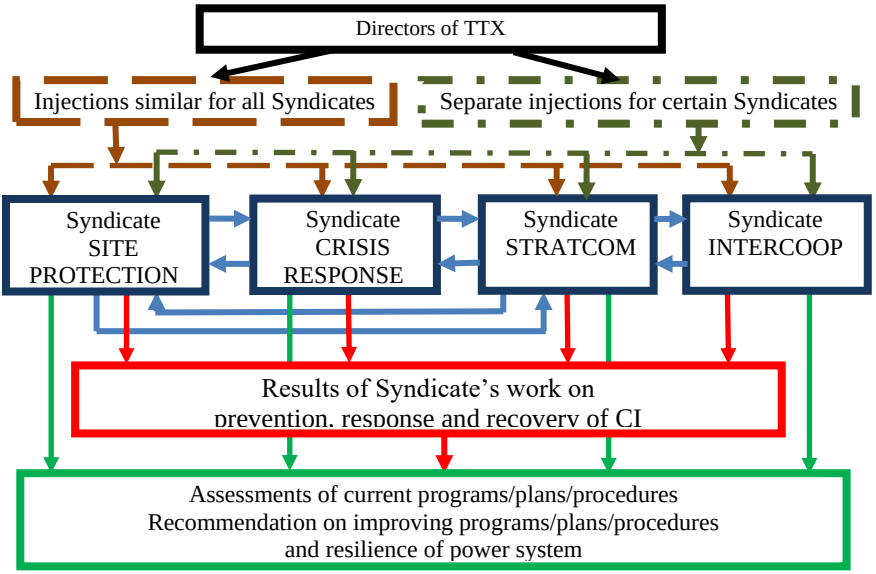

Figure 1: The general concept of injection introduction and syndicate's interaction.

The Reporting Stage had the aim to provide correct analysis of the TTX and evaluate the exercise against its stated aims and objectives as well as to identify the gaps in exciting plans and procedures (prevention of, protection from, mitigation of, response to, and recovery from a defined incident) as well as areas for improvement.

Lessons identified, in form of Evaluation Report, were presented to the Government of Ukraine as well as to NATO institutions. Thus, the Evaluation Report became a tool of increasing the Ukrainian authority's awareness of the contingency planning importance and would be transformed into working plan on removing gaps in the field. At the same time, the report enhanced NATO's competence in supporting nations in building resilience of CEI.

Overview of Results of TTX CORE 2017

The TTX CORE 2017 proved to be an effective tool to engage different institution into process of evaluation and assessments existing capacities of the state and society to match modern challenges in the field of CIP.

Participants highlighted next main positive points from training in form of TTX:

- Scenarios matched challenges faced by Ukraine;
- TTX provided opportunities to work and make decisions on their own in a stress-free environment;
- Ukrainian participants proved their interest in improving existing plans and procedures in the field of CIP;
- Gaps and inconsistencies in regulatory and legal framework for protection of critical infrastructure were identified;
- The involvement of foreign participants created the opportunities to get acquainted with the best practices of other countries in the field;
- A new approach to training was presented, with opportunities for networking and interagency involvement;
- There is a need to continue such type of training with a focus on some specific tasks;
- It was recognized that there needs to be greater state-private partnerships, especially in regard to information exchange and interaction during crises.

Among the main recommendations for Ukraine are:

- Accelerate the implementation of the National Security and Defense Council Decision on Critical Infrastructure;
- Regulate the interactions between state, private stakeholders and military command during crises;

- Establish procedures for information exchange related to threats (to include restricted data access) during crises;
- Codify by law the liability of private companies for security procedures, interaction with state authorities on the security of infrastructure facilities;
- The nuclear industry could serve as example to emulate in other areas of critical infrastructure protection (vulnerability assessments, protections plans, response plans);
- Establish a government crisis management and critical infrastructure protection center under Ukraine's Cabinet of Ministers; Include a sectoral situational crisis center under the Ministry of Energy and Coal Industry;
- Ensure absolute separation of different networks (SCADA from office networks).

Conclusion

The exercise in fact became an effective tool to build interagency networking and to establishing common understanding of the main problems that have to be resolved. TTX has helped to build the understanding that an effective cooperation between the government and the private sector is needed for enhancing resilience of national critical infrastructure. The training has helped to start the process of building common language between different institutions regarding the response to threats to critical infrastructures.

At the same time, the TTX has demonstrated that Ukraine needs effective governance, at a national level, at industry and individual organization level, to set goals and monitor progress towards them. The Government has to take the leading role in establishing the State CIP system including through approving Concept for building a state CIP system in Ukraine and appointing responsible body for its implementation. Particular tasks of a CIP system differ from the tasks of the existing state systems (civil defense, counter-terrorism, cyber threat counteraction, etc.) and that is why the establishment of a National Center for Crisis Management and Critical Infrastructure Protection as a separate body to be responsible for coordination and exchange of information is needed.

References

[1] Dmytro Biriukov, Sergiy Kondratov, Oleg Nasvit. and Oleksandr Sukhodolia, eds., *The Green Paper on Critical Infrastructure Protection*: *Analytical Report*

(Kyiv: NISS, 2015), http://en.niss.gov.ua/content/articles/files/Green-Paper-engl-4bd7c.pdf, accessed December 1, 2017.

2 "On Improvement of the Measures to Ensure Protection of Critical Infrastructure Objects," Decree of President of Ukraine no. 8/2017, 2017 (in Ukrainian), http://www.president.gov.ua/documents/82017-21058, accessed December 1, 2017.

3 "Homeland Security Exercise and Evaluation Program," FEMA (Official website of the Department of Homeland Security), last modified June 17, 2016, https://www.fema.gov/media-library/assets/documents/32326, accessed May 13, 2018.

4 Oleksandr Sukhodolia, "The Energy Dimension of War: An Overview of the Ukrainian Events in 2014–2016," *Energy Security: Operational Highlights* 11 (2017): 25-34, https://issuu.com/natoenseccoe/docs/operational_20highlights_20no_2011_, accessed November 20, 2018.

About the Author

See p. 119 in the previous article, https://doi.org/10.11610/isij.4108.