Coherent Resilience 2020
CORE20
Tabletop Exercise
Final Exercise Report

13-17 September 2021
Odesa, Ukraine

21 April 2022
NPS EAG , ENSEC COE

Table of Contents


CORE
2020
13-17 September 2021, Odessa, Ukraine
Enhance Resilience in Light of Hybrid Risks to Critical Infrastructure and Energy Systems
NPS
CCDCOE
Hybrid CoE

1. Introduction

1.1. Coherent Resilience Program

Coherent Resilience (CORE) is a series of national and regional level tabletop exercises (TTXs) developed by the NATO Energy Security Centre of Excellence (ENSEC COE) aimed at enhancing resilience of energy systems in an era of hybrid threats. CORE TTXs have been conducted in Ukraine as well as national and regional level programs in the Baltic States since 2014. CORE 20 was the second Ukraine CORE TTX and its development was approved by the NATO-Ukraine Platform on Countering Hybrid Warfare and Ukraine for European and Euro-Atlantic Integration.

1.2. Coherent Resilience 20 (CORE 20) Ukraine

1.2.1. Overview

In recognition of the strategic importance of the Black Sea region to NATO and its partners, NATO Foreign Ministers decided to enhance practical support to Ukraine related to the Black Sea including cooperation with the Ukraine Navy, situational awareness, port visits, exercises and sharing of information. The CORE 20 TTX was planned as a part of this support with the goal of developing Ukraine's resilience against hybrid risks and its crisis response capabilities by enhancing inter-agency and civil-military coordination, planning and preparedness. After several postponements due to COVID-19, the event was executed 13-17 September 2021.

1.2.2. Purpose, Aim, Objectives

CORE20 tabletop exercise was developed with the support of the NATO HQ Political Affairs and Security Policy Division (PASP), NATO HQ Emerging Security Challenges Division (ESC), the Energy Security Centre of Excellence (NATO ENSEC COE) and Cabinet Ministers of Ukraine to contribute the national authorities of Ukraine in building resilience through improved emergency preparedness, planning, prevention, and threat response. Additionally, CORE20 aimed to strengthen Ukraine's capability to protect critical infrastructure, maritime and cyber domains, and energy systems.

The aim of the Black Sea region focused TTX was to further capabilities of Ukrainian national and local authorities in crisis response and to enhance resilience in light of hybrid threats to critical infrastructure and energy systems through effective inter-agency coordination, civil military coordination, planning, preparedness and public-private cooperation.

The following objectives were identified for CORE 20:

- Assess resilience of Ukraine's critical infrastructure and preparedness against hybrid threats (disinformation, cyber-attacks, sabotage, covert operations);

- Validate the effectiveness of national crisis management plans, policies and procedures to respond to and mitigate the effects and possible impact of hybrid actions (to include energy supply);

- Exercise plans to heighten security of critical infrastructure and supply chains to include the General Staff among others;

- Evaluate strategic communications procedures to mitigate the influence of malign disinformation, including crisis communications strategies, plans and frameworks;

- Assess capability to coordinate with NATO members, partner nations and international organizations

1.2.3. Concept for the Event

CORE 20 was opened by welcome messages from the Director of the NATO Energy Security Centre of Excellence – Col. Darius UŽKURAITIS, and the Head of NATO Division (Defence and Security Aspects) of the Government Office – Col. Serhii Verbytskyi.

During the Welcome Remarks, Col. Serhii VERBYTSKYI in Odesa, Ukraine.

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

Phase One of the academic seminar consisted of a series of expert presentations to better prepare participants for the TTX. Day 1 Lectures included the following topics: Hybrid Threats to Critical Energy Infrastructure, presented by Mr. Florian Encke and Mr. Julijus Grubliauskas (both from NATO HQ); The Target of Hybrid Attacks: Critical Infrastructure, presented by Dr. Oleksandr Sukhodolia (National Institute for Strategic Studies, Ukraine); International Law and Hybrid Warfare, presented by Dr. Hanna Shelest (Head of Security Programmes, Foreign Policy Council "Ukranian Prism"), Cyber Security of Critical Infrastructure, presented by Dr. Oleksandr Potii (Deputy Head of the State Service for Special Communications and Information Protection) and Mr. Valentyn Petrov (National Security and Defense Council of Ukraine); and International Law and Hybrid Warfare, presented by Mr. Sergii Karasov (Lano Solutions).

During the seminar portion of the CORE 20 – Black Sea TTX program, participants and facilitators listen to subject matter experts present on topics such a strategic communications and cyber security.

Day 2 Lectures of the academic seminar included: Maritime Aspects of Hybrid Threats, presented by Lt. Alexandru Hudisteanu (Romania Navy, NATO Maritime Security Centre of Excellence); Counter Hybrid Actions by Military and Non-Military Organisations (National Security and Defense), presented by Capt. Stepan Yakymiak (Ukraine, National Defence University of Ukraine); Strategic Communications and Hybrid Threats, presented by Col. Douglas Cochran (1 German – Netherlands Corps); The Main Information Operations of Kremlin in Ukraine since 2014, presented by Ms. Liubov Tsybulska (Ukraine Crisis Media Center); Cyber Resiliency, presented by Maj. Emre Halisdemir (Republic of Türkiye, NATO Cooperative Cyber Defence Centre of Excellence); Practical Models for Interagency and International Cooperation in Countering Hybrid Threats, presented by Mr. Oleksandr Danylyuk (Centre for Defense Reforms, Kyiv) and

CORE20 TTX Introduction, presented by LCDR Özgür DÜNDAR (Republic of Türkiye, NATO Energy Security Centre of Excellence). At the conclusion of the Academic Seminar on Day 2, the TTX Scenario was presented by LTC Cezary Kozlowski (Republic of Poland, NATO Energy Security Centre of Excellence).

Phase Two of CORE 20 was the execution of the two-day TTX, the main event of the five-day program. Participants were assigned to one of five different syndicate groups:
(1) CIP against Hazards, Threat and Attacks syndicate was facilitated by Dr. Oleksandr Sukhodolia (National Institute for Strategic Studies, Ukraine), Mr. Pawel Kasprzyk (Republic of Poland, European Hybrid Centre of Excellence),
(2) Cyber Security syndicate was facilitated by Mr. Oleksandr Bakalynskyi (Ukraine, State Service of Special Communication and Information Protection of Ukraine) and Maj. Emre Halisdemir (Republic of Türkiye, NATO Cooperative Cyber Defence Centre of Excellence),
(3) Maritime Security syndicate was facilitated by Capt. Stepan Yakymiak (Ukraine, National Defence University of Ukraine), Capt. Ertürk Avcı (Republic of Türkiye, NATO Maritime Security Centre of Excellence) and Alexandru Hudişteanu (Romania Navy, NATO Maritime Security Centre of Excellence),
(4) Strategic Communications (STRATCOM) syndicate was facilitated by Ms. Liubov Tsybulska (Ukraine Crisis Media Center), Col. Douglas Cochran (United Kingdom, 1 German – Netherlands Corps) and Lt.Col. Annie Geisow (United Kingdom, NATO Strategic Communications Centre of Excellence),
(5) International Response/International Law syndicate was facilitated by Dr. Hanna Shelest (Head of Security Programmes, Foreign Policy Council "Ukranian Prism") and Mr. Sergii Karasov (Lano Solutions).

Phase Three of CORE 20 consisted of the TTX After Action (Hot Wash) and coincided with the Distinguished Visitors' Day. This phase allowed each Syndicate to have presenters brief their syndicate assessment and response to a selected inject and highlight overall syndicate outcomes regarding identified areas for improvement and best practices. Distinguished visitors consisted of an impressive group of senior officials, diplomats, and industry representatives. Participants were addressed by Olha Stefanishyna, the Deputy Prime Minister for European and Euro-Atlantic Integration.

1.2.4. The Final Exercise Report

This report focuses largely on syndicate responses to scenario vignettes and injects to include capturing key takeaways – areas of improvement, best practices, and recommendations. The next chapter of the report provides the exercise scenario. Follow-on chapters provide reports for each syndicate where a summary of responses to each vignette and inject are provided as well as key take aways. Due to relevance and/or time constraints, not every inject was addressed by each syndicate. As well, there are some differences regarding syndicate approaches to report development. The concluding chapter captures the broader key takeaways that are relevant beyond one syndicate.
Readers will note that the exercise was based on a fictional scenario that closely resembles regional realities, so syndicate responses are completed in line with the scenario, but key takeaways are provided without reference to the fictional countries etc.
Exercise evaluators captured and provided draft syndicate responses and key takeaways that were reviewed, refined, and expanded upon during a post exercise discussion conducted in Kyiv, Ukraine from

8-9 November 2021, where several facilitators, participants, and evaluators gathered to develop much of the final content of this report – it was a team effort.

2. CORE 20 Tabletop Exercise Scenario

2.1. Background and Scenario

The presented scenario is direct from the exercise planning documents and was presented to TTX participants.

2.2. Geopolitical Situation

Geopolitical tensions between two former countries of the Ponuxin Empire: Bastan and Senta, continued to influence the geopolitical situation in the region. The imperial expectations of Bastan constituted reasons for Bastan's constant attempts to destabilize Senta politically and economically. The main aim of Bastan's actions was to revive the former Ponuxin Empire under the so-called Union of Allied States, where Senta would be under full governance and rule of Bastan as the latter would acquire the regional dominance with the gained territory and resources of neighboring states. The central strategic peninsula in the Noir Sea belonging to Senta remained occupied by Bastan.

The general perception of the EU and NATO by Bastan was more negative as the EU and NATO expansions undermine Bastan regional integration plans. The EU was viewed as a competitor to future Union of Allied States. NATO was regarded as an aggressive organization that removes regimes which support Bastan's reintegration efforts within the Union of Allied States.

2.3. Socioeconomic Situation

Recently, Senta experienced a pro-European manifestation and eventually a people's revolution that ousted corrupt President and Government officials supporting Bastan's politics. As a result, a new government was elected with clear pro-European aspirations and objective to join the EU and NATO.
Due to previous political turmoil and high corruption, the economy of Senta was struggling, though recent years showed the start of a stabilization period. At the same time, pandemic-related challenges slowed down the economic growth both in Senta and in other countries. The high level of unemployment led to social tensions. The growing number of protests in the streets was driven by the absence of efficient reforms in the economic system, monopolization of energy markets by local oligarchs, high level of natural and human-made risks as a result of the depreciation of critical infrastructure in the country due to its long period of use.

The transport sector of Senta, in particular its port industry, was a significant driver of the economic development of the country and a foreign trade gateway. For example, 20 percent of the country's GDP was generated by the port. Two hundred thousand employees were employed in major seaports. In addition, ports accounted for 70 percent of Senta's exports and 65 percent of its imports. Ports of Senta were the crucial element of the country's logistics infrastructure, constituting the most powerful port potential among all countries of the Noir Sea region as almost half of all loaded containers in the Noir Sea were processed in the terminals of Senta. Nevertheless, the Bastan government's increasingly aggressive actions in the maritime domain disrupted the effective utilization of port potential, making the economic situation worse.

Import and export capacities of Senta's energy resources were connected with the port infrastructure in the Southern part of Senta. Odesa Sea Port, as well as Sea Port Pivdennyi, Chornomosk and Mykolaiv Sea Ports, were significant sea-gates for energy supplies and chemical products in the region. The abovementioned ports also constituted an essential part of Senta oil and gas transshipment and storage facilities.

Recently, the presence of significant oil and gas reserves in Senta's EEZ was confirmed. Their development could provide a better energy security level and become a source of stable financial growth for Senta. Moreover, Senta has the potential to become one of the top gas and oil producers in the region. New FDI in the oil and gas upstream sector is expected to grow significantly in the next few years. Major oil and gas companies, both local and foreign, obtained licenses and started exploration works, planning to begin oil and gas drilling activities in Senta's EEZ in the Noir Sea.
Moreover, the offshore part of Senta's EEZ in the Noir Sea was considered as one of the best locations to install wind power generators.

2.4. Weather and Gas Demand Situation

Senta experienced one of the coldest winters in history. The temperature was unusually low for the third week since the middle of December. It continually stayed at -20 °C level and reached -35 °C in some areas. The Noir Sea became increasingly icy, especially on the coastline and the marine traffic in those areas was possible only with the help of tug-boats.

Wind speed reached 40 m/s, while in some areas, the rate of 50 m/s was recorded. Severe wind conditions disrupted Senta transshipment operations. Ferry ships had to stay on the roadstead for a considering time while waiting for the weather to improve.

Heating season was at its peak. Gas demand reached historically high volumes, not observed before in Senta. Heat suppliers who were using biomass switched to gas to satisfy the heat demand under extreme cold weather.

The domestic gas demand registered on January 4 was 10 MCM/day in the Odesa region and 6 MCM/day in the Mykolaiv region.
The transit[1] of gas through Senta's territory to neighboring countries was in full capacity.

2.5. Critical Infrastructure Security in the Region

The overall structure of electricity generation, distribution and supply in the Southern region of Senta was displayed by analogy with the system of a real country – Ukraine.

Senta's electricity generation, supply and distribution infrastructure formed the united energy system (UES) – a set of power plants, electric networks, other objects of electric power, the combined standard mode of production transmission, and distribution of electric energy with centralized management of regime.

With the UES, Senta provided reliable and efficient energy supply to consumers all over the country and cross-border to keep the high level of energy security of the country.
The following power plants ensured the security of the electricity supply in the Southern region of Senta:

- South Senta Nuclear Power Plant – 3000 MW;
- Dnistrovska Hydroelectric Pumped Storage Power Plant – 972 MW;
- Tashlytska Hydroelectric Pumped Storage Power Plant – 302 MW;
- Odesa Thermal Power Plant – 68 MW;
- Mykolaiv Thermal Power Plant – 40 MW.

[1] In December 2019, Senta and Bastan signed a new 5-year contract for the transit of Bastan gas through the territory of Senta. According to the agreement, the volume of transit was reduced to 65 billion cubic meters per year in 2020 and further down to 40 billion cubic meters per year in 2021-2024.

It was essential to mention that Dnistrovska Hydroelectric Pumped Storage Power Plant covered 90 percent of the demand of the Odesa region.

The Odesa and Mykolaiv regions on the South of Senta were important electricity cross border supply areas from Bastan to Vela and Romania through the powerline transmissions of 330 kV and 400 kV. The main electricity interconnection between Senta and Vela was with CERS Moldova – 2520 MW (Молдавская ГРЭС), which was located on the Vela's territory.

The gas infrastructure was highly developed in the Southern region of Senta: there were 58 major gas transmission stations and 100 gas metering points. The significance of the gas supply in the area was high as gas was used nationwide in manufacturing and industrial spheres as well as by the state-funded organization. Gas was second on the list of the most consumed resources during the heating season.

The leading gas transmission company in the Odesa region was Odesa gas, which had under its governance 440 gas transmission stations and over 12318.6 km of gas pipelines.

Despite reduction in natural gas transit through the territory of Senta under the terms of the new 5-year contract with Bastan, the Southern region of Senta remained necessary for Bastan's gas transit to Vela and Romania. Odesa and Mykolaiv regions served as important territories where the Southern gas transit pipeline passes from Bastan to Vela and Romania. Thus, Senta played a crucial role in the gas supply to the countries of the EU.

The following installations were central in the Senta-Vela gas transit infrastructure:

- Berezivka, Pavlohrad and Marivka gas compressor stations of Southern gas transit corridor;
- Transboundary points of connection: Hrebenyky, Caushany, Orlovka (located in the Senta-Vela-Romania gas corridor in the territory of Senta).
-

There had been a discovery of significant gas deposits located in Senta's EEZ in the Noir Sea. After the exploration work, several new jack-up drilling rigs were installed within deposit occurrence: Odesa, Shtormov and Halitsyno. However, after Bastan's seizure of Senta's oil and gas fields in the Noir Sea along with infrastructure and equipment used for their development and supply to consumers, this part of the shelf was under Bastan's control.

The availability of new, adjacent oil and gas areas within Senta's EEZ in the Noir Sea (Delphin area) determined the feasibility of their development, obtaining economic income and improving the level of security of Senta's energy supply.

Odesa was used as a significant maritime transport hub. Two storage facilities were located in the city: Odesnafteprodukt and Eksimnaftoprodukt.

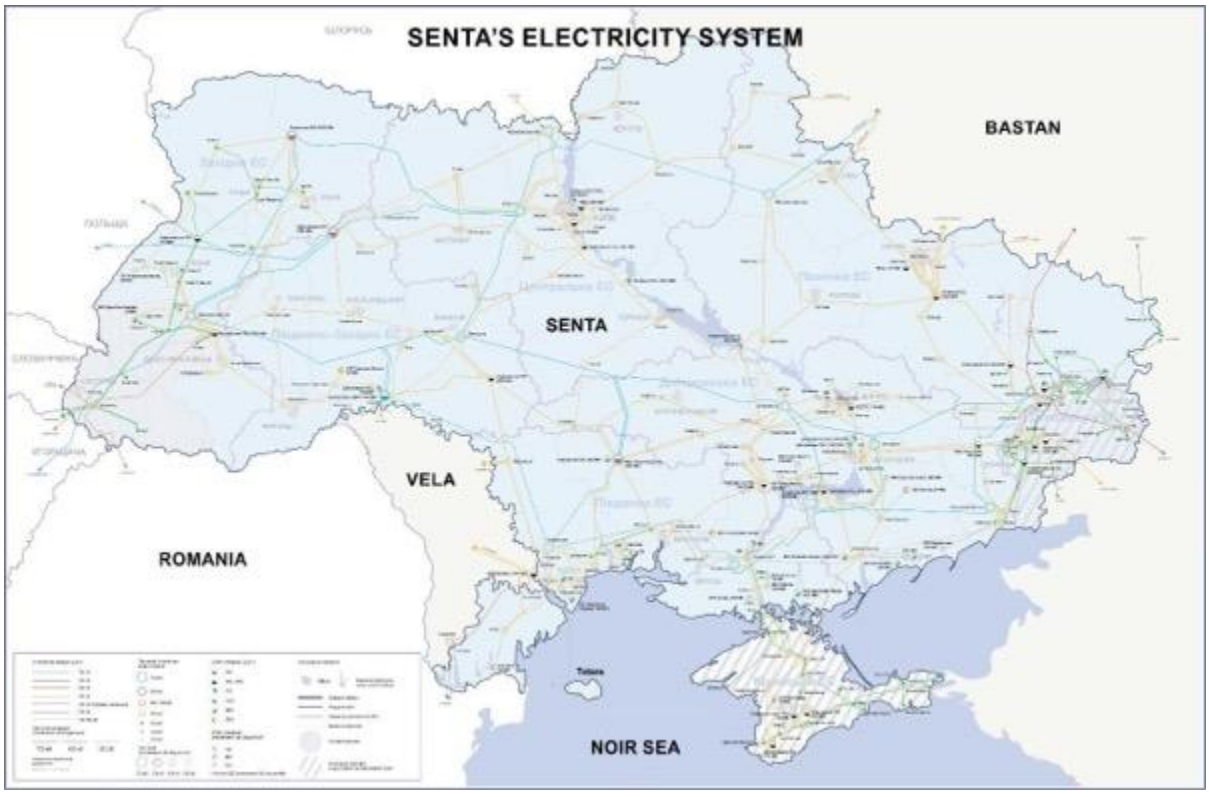
Seaports of Senta constituted the central part of the transshipment infrastructure of the state. The main shipping lines went through Odesa Sea Port, Mykolaiv Sea Port, Sea Port Pivdennyi and Chornomorsk Sea Port. The leading oil, gas and chemical products' handling and storage infrastructure were located in the following ports:

- Odesa Sea Port – sea oil and gas terminal;

- Sea Port Pivdennyi – ammonia gas transshipment base, sea oil terminal Pivdennyi (Ukrtransnafta), private-owned terminals, including TIS Company;
- Mykolaiv Sea Port – coal and oil transshipment base;
- Chornomorsk Sea Port – sea oil and gas terminal, Sulphur processing department.

Seaports of Senta constituted crucial importance in the cargo and passenger transshipment between Senta and other neighboring states. It is in Odesa ports where the transshipment of Senta's metal products takes place. The previous year the Odesa Sea Port turnover reached the index of 25,343 m tons. Besides, the ports of the Odesa region are the central locations for cereals, ore minerals, coal and cast-iron export transshipments.

Within the nearest vicinity of the southwestern coastline was the island of Totara, inhabited by approximately 12500 inhabitants in three main settlements. On the island, there was a maritime port and three drilling rigs. With the continental part of Senta, the Totara Island was connected via the Senta-Totara-Bulgaria Internet submarine cable, which was the primary source of the Internet for the entire Totara Island. There were eight gas and four oil jack-up drilling rigs in the waters surrounding the Totara Island, including those seized and controlled by Bastan.



2.6. Maritime Security Situation

The general maritime security situation in the Noir Sea had been deteriorating recently. Bastan's dominance in the Noir Sea has increased. Bastan undertook a rapid build-up of combat and enforcement

capabilities and began placing new and advanced surface combatants and submarines in the Noir Sea Fleet. Meanwhile, there had been a massive build-up of air and coastal defense cruise missiles on Senta's continental shelf, as well as growing Bastan electronic warfare capabilities.

The Bastan government repeatedly claimed that the breadth of Senta's EEZ was not measured correctly, in line with UNCLOS provisions, as large areas in the aforementioned maritime zone were the historic waters of Bastan and should have been fully under its imperative jurisdiction. Demanded areas are marked on the map below.

2.7. Cyber Security and Electronic Warfare

The overall cyber security situation is rather hostile. There have been reports of numerous cyber-attacks in the maritime and critical infrastructure spheres. Moreover, the websites of government officials, banks and leading news websites work with the periodical disruptions. Bastan gathers technical intelligence in Senta's information systems to collect information on vulnerabilities of Senta's public and corporate user systems that can be used for hacking, espionage and sabotage.

Moreover, most cyber- enables information operations target the national defence system. These attacks aim to polarize society, discrediting Senta's armed forces and diminishing trust in state institutions. Also, there has been an increasing number of ransomware attacks against Senta's state institutions as well as private and state companies.

The biggest threat for the disruption of Senta's critical infrastructure comes from cyber-attacks against industrial control systems (ICS), including in the energy and transport sectors. According to Senta's national security assessment, intelligence agencies of Basatan are especially active in trying to gain access and compromise critical infrastructures. This information corresponds to recent reports by international

cyber security companies who started revealing evidence of new cyber-attack malware with a code name 'Blackout' which specifically designed to take control of energy systems. 'Blackout' is a modified version of 'Industroyer' malware first identified in 201t, which was designed to attack electrix power control systems and systems and thought to have been behind the cyber-attack on Senta's power grid in 2016. Experts have noted Blackouts' ability not only to stay in the system and interfere with the operation of industrial control systems but also to compromise Safety Instrumented Systems (SIS), which make it one of the most dangerous new malware threats to industrial control systems since Stuxnet.

Electronic Warfare (further – EW) incidents are growing in the region. In recent years, Bastan has heavily invested in building EW capabilities in the Noir Sea region. Bastan's military and civilian vessels often use these capabilities. There have been reports of increasing satellite navigation problems for certain civilian and military ships, including major oil tanker in the Noir Sea, suggesting jamming and spoofing of GPS signals. Moreover, during the latest Bastan's naval exercise, satellite and communications were disrupted in southern parts of Senta.

2.8. Communication and Media Reports

The information environment is consistently hostile and under the substantial control of Bastan. There is a continuing campaign of dissemination of propaganda and disinformation, news fabrication by Bastan's news agencies and media outlets against Senta. The aim is to disparage Senta's statehood, discredit and provide disinformation about the government, and manipulate history and international legal provisions regarding the situation in the maritime zones of Senta.

To this end, Bastan is using available communications channels, including information channels of Senta, controlled by Bastan-backed actors. This hinders communication of official pro-European position of the Senta's government.

Bastan's disinformation activities are intended to decrease the level of population support regarding the economic and energy diversification reforms of Senta. Furthermore, Bastan propaganda creates images and tries to persuade Senta nation of the benefices of the membership in the Union of Allied States, where Bastan states that it would bring economic progress comparing to the membership in the EU and NATO.

Cyber-enabled defacement operations target Senta's governmental institutions and private companies. There attacks aim to polarize society, discredit Senta's armed forces, and diminish trust in state institutions. Creators of fake stories strive to be more compelling and use narratives that are more often based on actual events. These narratives are more widely spread in foreign media; new institutions and social groups are involved, facilitating the spread of disinformation.

The situation on the occupied territory of Senta concerning the freedom of speech is degrading. There are regular media reports about the violation of human rights and suppressing the civil activists' performance by Bastan's forces.

2.9. Scenario Conclusion

The scenario presented in this document was discussed during the "Scenario, vignettes and injects workshops" on October 2019 and May 2021 in Kyiv, Ukraine. It was reviewed, discussed and finally accepted by stakeholders.

This scenario was used to develop the vignettes and injects for the CORE 20 TTX.

2.10. Vignettes and Injects Section

Five separate Syndicates were developed, and - essentially – each Syndicate executed its own tabletop exercise with only limited differences in scenario injects. The five Syndicates each had representatives from the various ministries, security organizations, and energy industry as necessary to facilitate their focus area. The Syndicates were: 1. CIP Against Hazards, Threats and Attacks, 2. Cyber Security, 3. Maritime Security, 4. STRATCOM, 5. International Response/International Law.

The exercise was conducted in the light of hybrid threats that form a background for the scenario development. This includes the significant components of security of electricity and natural gas supply in the form of supply disruption, cyber and electronic attacks against critical infrastructure, maritime threats against shipping and ports infrastructure. The mixture of socioeconomic, geopolitical, strategic communication elements was considered as well.

This document presents vignettes and injects for the CORE20 TTX based on the scenario.

The timeline of the crisis evolution:
- crisis starts on January 6, 11:00, Year 20YY;
- crisis scenario continues for eight weeks until March 6.

2.11. Structure of Vignettes and Injects

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

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

Training audience will develop five vignettes for each scenario phase, and several injects for each vignette:

Vignette 1: Pre-conflict phase: hybrid influencing

The political and economic intimidation against Senta by Bastan authorities is growing. Based on the gas transit agreement, which has been signed by Bastan and Senta last year, the Bastan government accused Senta of infringing agreement provisions. Senta denies any violations. However, Bastan's media and some of Senta's media controlled by Bastan keep spreading the messages about Senta's infringement, stressing the importance of the corresponding agreement for Europe's energy security as the gas transit[2] to European countries is partially ensured through the territory of Senta.

The situation is aggravated by the fact that there is no new contract for gas supply between Bastan and Vela. Given disputes over contractual provisions, Bastan temporarily substantially reduces gas supplies to Vela. Vela maximally draws gas from the transit pipeline, limiting gas supplies to Senta's customers in the Odesa region, near the border with Romania.

Meanwhile, Bastan inflicted import restrictions on Senta's agriculture, manufacture, and metal products and fuel, chemicals, and petroleum products. Besides, Bastan ceases to supply oil products to Senta with automotive, railway transport, and pipelines.

Three websites were found on the Internet with identical visual designs and features of the official websites of Senta GTS Operator, PSG Operator, and Naftogaz Company. Moreover, e-mails with phishing features and having attached Microsoft Word documents have been found in the e-mail boxes of Senta's regional government agencies.

Media reports were released about the powerful cyber-attack on Liebherr's internal network in Germany. As a result, port cranes at the Poti Sea Port in Zestan have stopped working.

From the middle of December, Senta's coast guards regularly report about the Bastan's Navy presence in Senta's EEZ. It is reported that Bastan conducted military exercises in the Noir Sea in the nearest vicinity of the fairway passage of merchant and passenger ships from/to ports in the Odesa region.

Vignette 2: Low-intensity hybrid operations

Weather conditions in the Southern regions of Senta deteriorated at the beginning of February. The wind speed reaches 50 m/s index causing considerable damage, namely in the Odesa region.

Bastan's import restrictions on Senta's agriculture, manufacture and metal products, fuel, chemicals, and petroleum products contribute to the decline of Senta's economy, which has already been in recession. Pro-Bastan activists use the economic downturn as a chance to intensify protests against Senta's government. Social tensions reach their peak when news about Odesa City Council's decision concerning the secession of the Odesa region from Senta has spread via the Internet.

[2] The completion of new gas infrastructure projects in recent years allows Bastan to reorient most of gas supplies to Central and South Eastern European countries without using Senta's transit corridor.

The work of Odesa Sea Port is continuously disrupted by the actions of pro-Bastan activists and incidents in the cyber-security domain. Moreover, Senta's civilian and coast guard vessels reported technical issues in their navigation system.

Furthermore, Bastan's vessels act aggressively against Senta's fishing boats. Coast guard ships of Bastan intimidate and threaten cargo vessels of Senta and foreign states as well. Recently, Bastan Naval Forces provided support to the illegal gas exploration and drilling rigs installation operation within the territory of Senta's EEZ. The 24-hour security guard patrol of Bastan's Navy was established around the rigs.

Vignette 3: Conflict phase: High-intensity hybrid operations

Senta's critical infrastructure experiences a wide range of kinetic and non-kinetic attacks. Disruptions occur on the natural gas transmission pipeline in the Southern gas transit corridor, affecting supply to the Southern region of Senta and the neighbouring foreign states. Moreover, there is a threat of disruption of the heating season not only in the southern part of Senta but in the Kharkiv and Luhansk regions as well, in particular those heavily depending on the gas supplies from Bastan.

In the South of Senta, there is a one-third increase in the number of emergencies, fires, and accidents caused by arson and terrorist attacks using explosives, leading to a significant increase in the number of casualties. A notable incident is suspected in PJSC 'Odesa Portside Plant', where the considerable release of hazardous chemicals is reported.

Information on disruptions in the South Senta NPP operation is disseminated. Bastan's media blames Senta's authorities for the release of radiation. Almost simultaneously, information about the attack against hydroelectric pumped storage power plant attack is being spread.

Massive cyber-attacks disrupt the operation of the Odesa Sea Port, including transportation and cargo handling. The branches of Oshchadbank and PrivatBank banking systems in the Odesa region were attacked.

In a month after the first cyber-attack on Liebherr's internal network in Germany, there have been a series of minor cyber-attacks on Liebherr's port cranes all over Europe.

In the maritime domain, Bastan's Navy ships are increasing their presence in Senta's EEZ, using navy exercises and interrupting the international passenger and cargo sea transhipment.

Vignette 4: Hybrid warfare

Tensions between Bastan and Senta have reached the highest level ever. Senta's military intelligence reported an unprecedented number of military build-up in Bastan Navy's bases in the Noir Sea. A significant number of provocative accidents have started to occur on Totara Island. Reports of the loss of GPS and GSM signals on the island. The Internet connection on the island was disrupted.

At the same time, Senta continues to experience a growing number of cyber-attacks against governmental and local institutions and critical service providers. Bastan's and Senta's media aggressively reports about

the inability of Senta's central and local authorities to provide essential services for the population. Moreover, top commanders of Senta's armed forces in Kyiv and Navy officials in Odesa and Totara Island received e-mails from unconfirmed accounts with a direct warning 'not to follow orders of Senta's political authorities or they and their families will be in danger'.

Social media is full of reports and active discussions about the possible separation of the South part of Senta. The same news is being spread via official web pages of regional councils. The above leads to pressure inside governmental institutions, law enforcement agencies, and armed forces. In the last 24 hours, street manifestations against the Senta government intensified dramatically, namely in the central cities of southern regions: Odesa, Mykolaiv and Kherson. As a result, the government is overstretched, and the population is confused.

Against the background of significant cyber disruptions, psychological pressure, the spread of misinformation, and growing street manifestations in southern regions, suddenly, a considerable number of military forces without insignia launched on the Totara Island. The Port of Totara Island access is blocked by the cargo ships with no State flag identification. The access by water to Totara Island is cut off.
The drilling rigs for hydrocarbon production of Totara Island located in Senta's EEZ were occupied and now are under the full control of armed men with no State identification.

Vignette 5: Post crisis stabilisation

This vignette focused on the post-crisis and recovery stabilisation process. The post-crisis stabilisation takes place after the end of the crisis scenario – from March 7, 20YY. Crisis management issues are to be discussed, as well.

Vignette Notes

Each syndicate will be presented with several questions for the post-crisis stabilisation discussion.
Vignettes 1 through 4 contain injects for each of the five syndicates. Vignette 5 displays discussion questions for each of the five syndicates.

All events last 59 days, from January 6 to March 5 (the Pre-conflict phase lasts for 21 days, the Low-intensity hybrid operations continue for 28 days, the Conflict phase is six days, and the Hybrid warfare remains for four days).

Injects are grouped for each of 5 syndicates:

Syndicate 1 – CIP against hazards, threats and attacks;

Syndicate 2 – Cyber Security;

Syndicate 3 – Maritime Security;

Syndicate 4 – STRATCOM;

Syndicate 5 – International response / International law.

The training audience in all syndicates were equipped with the scenario, vignettes and injects, and a separately printed map of the Senta electricity system. Syndicate 3 (Maritime Security) were additionally equipped with four maritime maps (one for each of the vignettes 1-4) with the exact locations of events.

3. Syndicate 1: CIP against hazards, threats and attacks

Ukraine's National Institute for Strategic Studies, Dr. Oleksandr Sukhodolia, facilitated the Crisis Response Syndicate and presents a Vignette during the conduct of the CORE 20 TTX in Odesa, Ukraine.

3.1. Vignette 1: Pre-conflict Phase: Hybrid Influencing

Political and economic intimidation against Senta by Bastan authorities is growing. On the basis of the gas transit agreement, which has been signed by Bastan and Senta last year, the Bastan government accused Senta of infringing agreement provisions. Senta denies any violations. However, Bastan's media and some of Senta's media controlled by Bastan keep spreading the messages about Senta's violation, stressing the importance of the corresponding agreement for Europe's energy security as the gas transit to European countries is partially ensured through the territory of Senta.

The situation is aggravated by the fact that there is no new contract for gas supply between Bastan and Vela. Given disputes over contractual provisions, Bastan temporarily reduces gas supplies to Vela. Vela maximally draws gas from the transit pipeline, limiting gas supplies to Senta's customers in the Odesa region, near the border with Romania.

Meanwhile, Bastan inflicted import restrictions on Senta's agriculture, manufacture, and metal products, as well as fuel, chemicals, and petroleum products. Besides, Bastan ceases to supply oil products to Senta with automotive, railway transport, and pipelines.

Three websites were found on the Internet with identical visual designs and features of the official websites of Senta GTS Operator, PSG Operator, and Naftogaz Company. Moreover, e-mails with phishing

features and attached Microsoft Word text documents have been found in the e-mail boxes of Senta's regional government agencies.

Media reports were released about the powerful cyber-attack on Liebherr's internal network in Germany. As a result, port cranes at the Poti Sea Port in Zestan have stopped working. From the middle of December, Senta's coast guards are regularly reporting about the Bastan's Navy presence in the Senta's EEZ. It is reported that Bastan conducted military exercises in the Noir Sea in the nearest vicinity of the fairway passage of merchant and passenger ships from/to ports in the Odesa region.

Inject 1.1.1: Day 1: January 6, 11:00

A year after signing the gas transit agreement, Bastan's authorities accuse Senta of violating the agreement – warning to terminate the contract and halt gas supplies through Senta's territory.

Response to Inject 1.1.1

The participants' major concern was the country's ability to ensure adequate gas supply for winter heating. There were wide-ranging discussions about how various levels of government would respond to the threat, but it was unclear whether a specific ministry or commission would take the lead in addressing the issue. The syndicate leader was adamant that the issue was political and would require action by the Cabinet of Ministers. Alternative energy supplies were discussed; however, it was unclear what actions could be taken to address potential energy supply shortages. The syndicate agreed that convene an assigned interagency level war group approved by center authorities to assess the threat and develop a response was the most prudent course of action.

Inject 1.1.2: Day 9: January 14, 13:00

Bastan announces blocking the exports of anthracite coal from Bastan and eastern Senta (occupied territory not under the control of Senta's government) to Senta, as well as bans the import of agricultural, metal, ferrous and nonferrous metal, chemicals, machinery, fuel and petroleum products from Senta citing alleged gross infringements of product quality requirements.

Response to Inject 1.1.2

This inject generated broad discussions of implications resulting from Bastan blocking coal imports and putting restrictions on Senta exports. Discussions included: alternative power supplies (conservation of resources, available reserves); civil unrest due to shortages; the possibility of a Bastan disinformation campaign designed to undermine Senta's government; the apparent lack of mechanisms to coordinate public-private sector responses to mitigate impacts and most importantly; the lack of a set of inter-related consistent, conceptual, legislative and regulatory plans and policies that provide a systematic approach to planning at all management levels, for all jurisdictions and all categories of stakeholders involved in responding to incidents and crisis situations resulting from all-hazards threats.

Participants also had extended discussions regarding identifying and protecting critical infrastructure. It was suggested that there should be a list of sites (strategic assets) identified by the national government that lays out the critical infrastructure at the local, regional, and national levels. It was discussed that military, police, and the national guard have the responsibility to protect strategic assets, however the discussion did not go into detail as to what the role of other first responder's roles would be in this regard. The survey comments identify several agencies with the role of protecting critical infrastructure. Participants were clear that the current situation in Ukraine, regarding the protection of critical infrastructure is exclusive to each agency's mission and responsibilities, making unified action at the national level virtually impossible.

Inject 1.1.3: Day 15: January 20, 10:00

Telecommunications equipment is partially disrupted (switches in the service provider's supply station to the seaport in Odesa), temporary lack of connection with critical infrastructure objects. Switching to the backup power system.

Response to Inject 1.1.3

The need to restore telecommunications connectivity was identified as a national priority. To mitigate loss of connectivity, participants immediate response was to use Senta's military to deal with the deteriorating situation. Participants discussed that Senta did not have a comprehensive database to identify and categorize critical infrastructure As the discussion proceeded, there was concern that the shift to the alternate supply chain would be required to keep critical infrastructure functioning, however it was not clear which government entity had the authority or capacity to deploy back-up generators. It also became apparent that Senta did not have a comprehensive database to identify and categorize critical infrastructure.

There were discussions about governmental roles and responsibilities. It was suggested that a Commission at State Level with representation from the appropriate ministries be formed to address the situation. The Prime Minister would head the technological and emergency situations group/commission (organization

exists but name does not easily translate) to analyze the situation, evaluate and decide on mitigation procedures, assign responsibilities, and prioritize actions. This entity is funded and has designated personnel assigned by respective ministries. As participants continued to discuss incident response options, it became clear that unity-of-action would be dependent on a comprehensive set of emergency and crisis response plans – something Senta did not have. The need to share information across all levels and government and across impacted critical infrastructure sectors was also identified.

Participants agreed that identifying the nature of the threat was crucial to deciding on an appropriate response. Attributing the disruption to a Bastan hybrid influencing campaign was key.

3.2. Vignette 2: Low-Intensity Hybrid Operations

Weather conditions in the Southern regions of Senta deteriorated at the beginning of February. Wind speed reaches 50 m/s index causing considerable damage, namely in the Odesa region.

Bastan's import restrictions on Senta's agriculture, manufacture and metal products, as well as fuel, chemicals and petroleum products contribute to the decline of Senta's economy which has already been in recession. Pro-Bastan activists use the economic downturn as a chance to intensify protests against Senta's government. Social tensions reached their peak when news about Odesa City Council's decision concerning secession of the Odesa region from Senta has spread via the Internet.

The work of Odesa Sea Port is continuously disrupted by the actions of pro-Bastan activists and incidents in the cyber-security domain. Moreover, Senta's civilian and coast guard vessels reported technical issues in their navigating system.

Furthermore, Bastan's vessels act aggressively against Senta's fishing boats. Coast guard ships of Bastan intimidate and threaten cargo vessels of Senta and foreign states as well. Recently, Bastan Naval Forces provided support to the illegal gas exploration and drilling rigs installation operation within the territory of Senta's EEZ. The 24-hour security guard patrol of Bastan's Navy was established around the rigs.

Response to Vignette 2

There was a prolonged discussion of attribution for the acts and whether the situation constituted a civil emergency or a state of war. The State Service of Special Communication and Information Protection representative stated that there was a need for strategic communications to the local populace regarding actions by the government to contain the evolving crisis situation and the challenge of staying ahead of the media to prevent panic and civil unrest.

Participants also noted that Local and Regional level commissions would be formed to address the situation. These commissions would provide advice to a national commission headed by the Prime Minister. One participant described the current decision-making process as very slow and centralized. Local Administration officials were confident they had the resources and capabilities to respond to the explosion and fire described in Inject 2.

A significant amount of time was spent discussing the need to implement martial law. There were concerns that if martial law was declared it may lead to further civil unrest. State Emergency Services representatives stated there were existing plans, decrees and regulations to deal with the emergency, but did not provide specific details.

Because the incidents involved multiple infrastructure sectors, participants were unsure which arm of the government would be responsible for managing the overall response. Also, there was concern amongst the participants that there might not be adequate resources or plans to deal with food, water, and energy shortages. There was in-depth discussion concerning reserve funds for resources to support response activities in the Odessa region. Participants were unsure how the request for and distribution of funds would be accomplished. They determined that a request would be submitted at the regional level for consideration by the Special Commission.

Participants determined that Liaison Officers (LNOs) would be required to facilitate interagency coordination, but training for LNO-specific duties did not exist. The point was made that Ukrainian territorial defense forces could assist with humanitarian assistance (HA), conduct internally managed military, civic action (MCA) and defense support of civil authorities (DSCA) programs, and provide support to civil administration (SCA) operations.

Inject 2.1.1: Day 22: January 27, 8:00

Under the pretext of deteriorating economic situation and rising prices for petroleum products and fuel, pro-Bastan activists start blocking main roads, port facilities, and fuel terminals in Odesa Sea Port. Unidentified persons cut off port telecommunications cables on a special communications cable network outside Odesa Sea Port's territory.

Response to Inject 2.1.1

To address the cut telecommunications cables, the participants identified that Odesa's Special Telecommunications Services (each region has this that fall under the State Service of Special Communications) would respond to fix cables and restore telecommunication services.

Police would lead the response to restore order with the support of the National Guard. This support does not require special approval at the national level. A legal framework exists to enable this support to be implemented immediately, however, the military does require special approval to obtain National Guard support. In this situation, the military would also be put on alert.

Inject 2.1.2: Day 26: January 31, 12:00

The explosion is heard in the Odesa Sea Port oil storage facility. Following the explosion, a big fire erupts in the territory of the OMTP Oil District. Some casualties are reported. The cause of the explosion is not confirmed.

Response to Inject 2.1.2

The Fire Security Department as the port would be the first entity to respond and assess the necessary support required to extinguish the fire and restore damaged facilities. The State Service for Emergency Situations would be notified, and the regional departments would also respond with medical and fire department support. The police would cordon the area and provide security.

The Security Service of Ukraine's counterterrorism unit would respond to conduct the investigation. If it is determined it was a terrorist attack, then it would fall under the Security Services for further response.
For this inject, the appropriate plans, policies, and procedures are in place to provide a comprehensive and effective response.

Inject 2.1.3: Day 28: February 2, 03:00

Small scale blackout occurs in the Odesa region. The initial assessment confirms that the transformers of several substations are physically damaged. Unverified reports claim that some gunshots were heard in the neighbourhood.

Response to Inject 2.1.3

Participants stated that technicians would respond to substations and attempt to restore electric services. If large scale, there may be a state of emergency declared in the Odesa region and the police and National Guard would respond. The State Security Service would also respond to conduct the investigation.

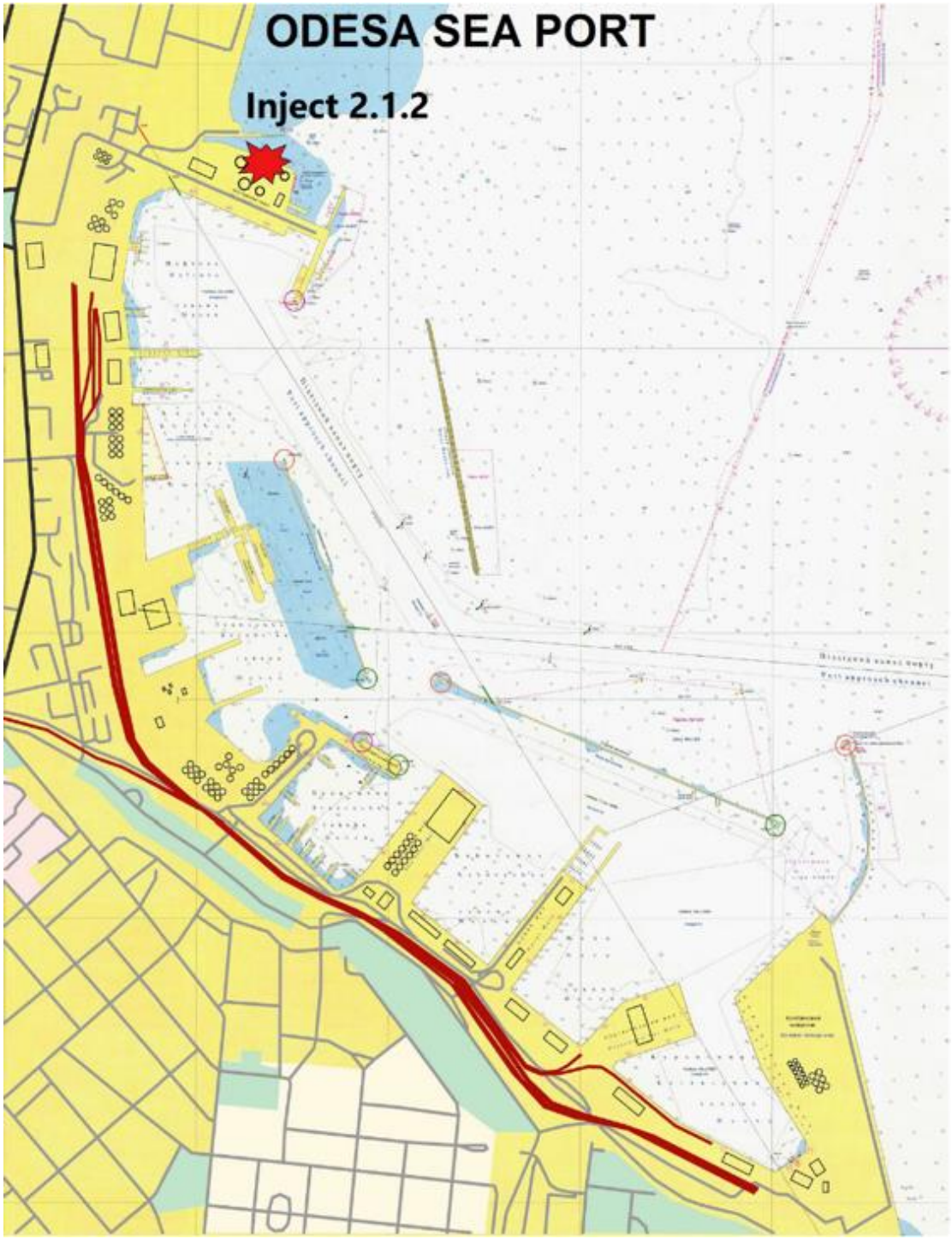
The regional technological and emergency situations group/commission headed by the Odesa regional governor would have an emergency meeting regarding the incident to identify further response and support requirements.

Inject 2.1.4: Day 36: February 10, 11:00

High levels of organic chloride contaminate the oil in the Southern Druzhba pipeline around Brody. Bastan accuses Senta of the deliberate act of sabotage. Given the connection of the Druzhba pipeline with the Pivdennyi terminal via Odesa-Brody, oil supplies through this terminal are significantly affected.

Response to Inject 2.1.4

Participants highlighted that it is impossible to contaminate the oil because the operator would see if something happens instantly and this would be the responsibility of Ukrenergo.


ODESA SEA PORT
Inject 2.1.2

3.3. Vignette 3: Conflict Phase: High-intensity Hybrid Operations

Senta's critical infrastructure experiences a wide range of kinetic and non-kinetic attacks. Disruptions occur on the natural gas transmission pipeline in the Southern gas transit corridor, affecting supply to the Southern region of Senta and the neighbouring foreign states. Moreover, there is a threat of disruption of the heating season not only in the southern part of Senta but in Kharkiv and Luhansk regions as well, in particular those heavily depending on the gas supplies from Bastan.

In the South of Senta, there is a one-third increase of the number of emergencies, fires and accidents caused by arson and terrorist attacks using explosives, which in turn has led to a significant increase in the number of casualties. A significant incident is suspected in PJSC 'Odesa Portside Plant' where the considerable release of hazardous chemicals is reported.

Information on disruptions in the South Senta NPP operation is disseminated. Bastan's media blames Senta's authorities for the release of radiation. Almost at the same time, information about the attack against hydroelectric pumped storage power plant attack is being spread.

Massive cyber-attacks disrupt the operation of the Odesa Sea Port, including transportation and cargo handling. The branches of Oshchadbank and PrivatBank banking systems in the Odesa region were attacked.

In a month after the first cyber-attack on Liebherr's internal network in Germany, there have been a series of minor cyber-attacks on the Liebherr's port cranes all over Europe.

In the maritime domain, Bastan's Navy ships are increasing their presence in the Senta's EEZ, using navy exercises and interrupting the international passenger and cargo sea transhipment.

Response to Vignette 3

TSO representatives noted that technical SOPs exist for handling drops in gas pressure, and that they had been successfully employed during real world situations. There was debate about incident response authorities and responsibilities for fire and HAZMAT incidents. Also, Local Administration representatives seemed confident they could handle the tactical situation i.e., HAZMAT operations and evacuations. Discussions revealed confusion about which agencies or ministries were responsible for identifying, prioritizing and protecting critical infrastructure.

There were lengthy discussions about declaring martial law and the implications for civil strife if it were approved.

Discussions concerning nuclear power events centered mainly on determining the cause of the shutdown and identifying alternative power sources.

Responsibilities for damage assessments resulting from possible attacks were discussed. There was debate about whether the armed forces or another agency had responsibility for counter-UAV operations; it was not resolved. There was a brief discussion of reaching out to the international community for disaster aid assistance, civic action and defense support of civil authorities (DSCA) programs, and provide support to civil administration (SCA) operations.

Inject 3.1.1: Day 52: February 26, 5:00

The Gas Transmission System Operator of Senta (GTSOU) observes rapid pressure drop at several gas metering stations: Hrebenyky (Senta-Vela interconnector) and Kaushany (Vela-Senta interconnector). The physical flow of gas via the Southern part of Senta and Vela is interrupted, leading to a reduction in gas supply to individual districts of the Odesa region, nearby Romania border.

Response to Inject 3.1.1

Governmental owned gas companies would increase gas extraction from the sea. There would also be a heightened security posture for pipeline protection. Operators would also switch to energy conservation mode where feasible. Key production facilities and gas providers will be identified for higher priority, so others would be severely limited or even cut to zero.

Inject 3.1.2: Day 54: February 28, 08:00

Major explosions at Ammonia production and storage facilities in PJSC 'Odesa Portside Plant'. Significant release of ammonia and other hazardous chemicals in the atmosphere as a result of the explosion. Dozens of casualties are reported in the plant. The toxic cloud of ammonia is heading towards Odesa city and neighbouring towns.

Response to Inject 3.1.2

The Odesa region technological and emergency situations group/commission will declare for an evacuation of the population from the region, coordinate the evacuation, and deal with the consequences at the explosions site (casualties and damage). Regional public transportation assets would be used to support evacuation efforts. Police would maintain order and conduct traffic control. There is internal regulatory frameworks that exists for critical infrastructure sites to include these storage facilities. On the regional level, the critical infrastructure response plan exists and would be implemented.

Inject 3.1.3: Day 54: February 28, 17:00

There are significant delays in the unloading and loading of ships in the ports of Odesa, Chernomorsk, Yuzhny, Kherson. Deliveries of coal that have already been ordered have been ceased. The shortage of coal and other fuels leads to a reduction in heat and power generation, and in some regions of the country, to a complete cessation of electricity generation.

Response to Inject 3.1.3

The region's nuclear power plant would increase power generation production. Also, hydropower production plants can also increase production and support the region. The coal and actual fuel deliveries are not critical. Energy supply would be prioritized to critical infrastructure sites. Non-critical sites will divert energy to the critical facilities. The region can sustain itself in this situation.

Inject 3.1.4: Day 55: March 1, 11:00

South Senta Nuclear Power Plant is suddenly forced into an emergency shutdown. Bastan media blame the US nuclear fuel supplier and Senta's 'corrupted authorities' reports that a significant incident occurred in the nuclear power plant with an essential release of radiation.

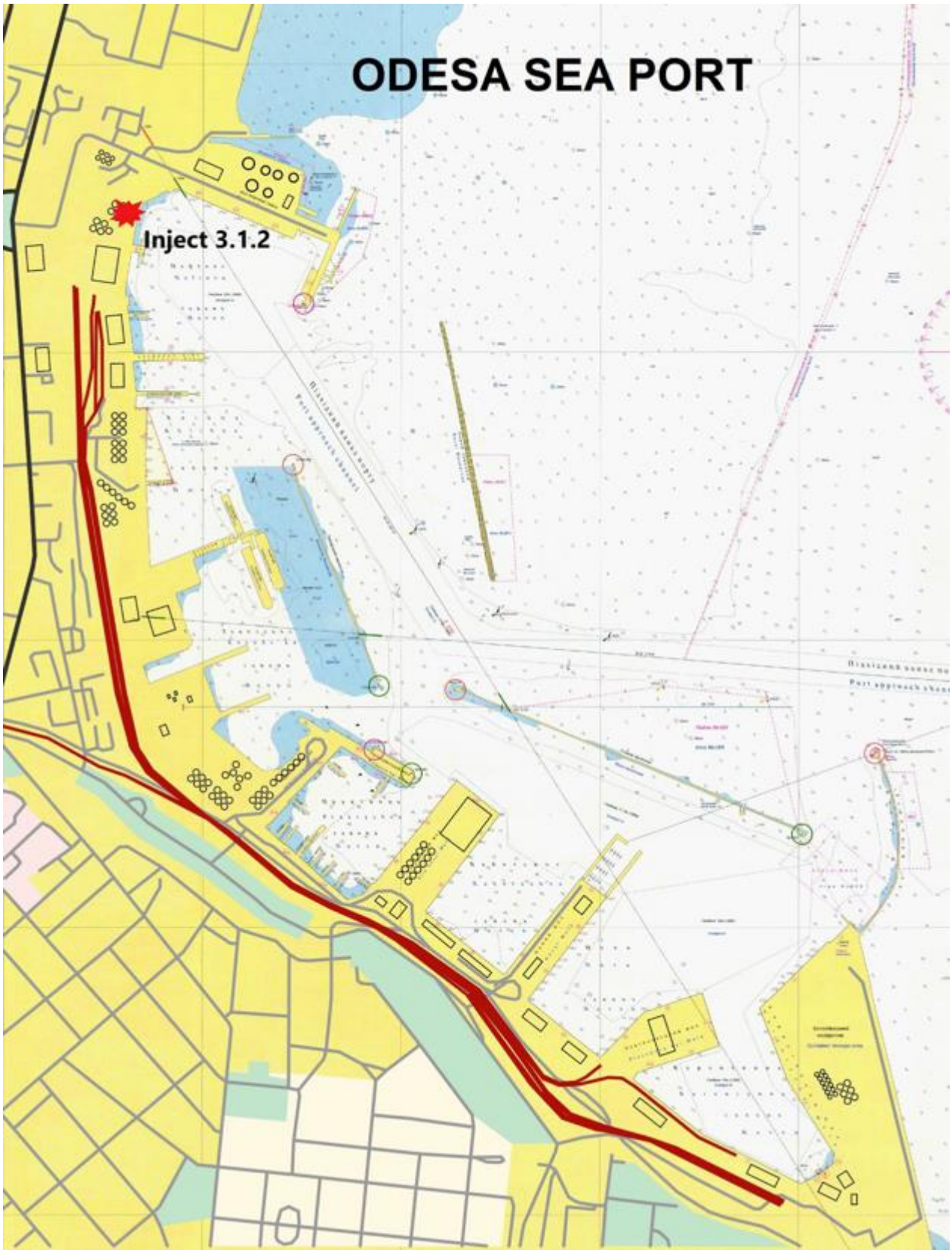
Response to Inject 3.1.4

The capability exists to restore operations at the nuclear power plant should the shutdown have taken place. In this case, it appears that this was a normal maintenance issue that the adversary attempted to exploit with a disinformation campaign. The local population would be informed of the fake news and proper restoration.

Inject 3.1.5: Day 55: March 1, 12:30

Dnistrovska hydroelectric pumped storage power plant is reportedly attacked using low altitude drone swarms. The engine room is damaged. The hydroelectric power station is disconnected from the grid. Uncontrolled leakage of water from the reservoir begins.


Inject 3.1.5
Dnistrovska Hydroelectric
Pumped Storage Power Plant
SENTA
VELA
Inject 3.1.4
South Senta Nuclear
Power Plant
Inject 3.1.1
Hrebenyky GMS
Kaushany GMS
Senta territory
under
Bastan occupation
ROMANIA
Totara


ODESA SEA PORT
Inject 3.1.2

Response to Inject 3.1.5

First, medical support would be provided to casualties. A counter-terrorist operation would be declared after an initial investigation. Vela would immediately be notified as there would likely be dangerous flooding and requirements for evacuation. An assessment would need to be made on whether people in the local region may also require evacuation.

On site technicians would implement mitigation measures in an attempt keep damage to a minimum as much as possible. The State Service for Emergency Situations would deploy technicians to site to begin necessary repairs.

This incident will effect the entire country, so other regions implement alternative power distribution and realign resources according to established priorities and plans. More likely to be targeted critical infrastructure would receive increased security measures to include counter-drone capabilities and deployed forces. Other critical infrastructure would also heighten security with enhanced patrols etc.

3.4. Vignette 4: Hybrid Warfare

Tensions between Bastan and Senta have reached the highest level ever. Senta's military intelligence reported an unprecedented number of military build-up in Bastan Navy's bases in the Noir Sea. A significant number of provocative accidents have started to occur on Totara Island. Reports of the loss of GPS and GSM signals on the island. The Internet connection on the island was disrupted.

At the same time, Senta continues to experience a growing number of cyber-attacks against governmental and local institutions, and critical service providers. Bastan's and Senta's media aggressively reports about the inability of Senta's central and local authorities to provide critical services for the population. Moreover, top commanders of Senta's armed forces in Kyiv and Navy officials in Odesa and Totara Island received e-mails from unconfirmed accounts with a direct warning 'not to follow orders of Senta's political authorities, or they and their families will be in danger'.

Social media is full of reports and active discussions about the possible separation of the South part of Senta. The same news is being spread via official web pages of regional councils. The above leads to pressure and tensions inside governmental institutions, law enforcement agencies, and armed forces. In the last 24 hours, street manifestations against the Senta government intensified dramatically, namely in the central cities of southern regions: Odesa, Mykolaiv and Kherson. As a result, the government is overstretched, and the population is confused.

Against the background of significant cyber disruptions, psychological pressure, the spread of misinformation, and growing street manifestations in southern regions, suddenly a considerable number of military forces without insignia launched on the Totara Island. Access to the Port of Totara Island is blocked by the cargo ships with no State flag identification. Access by water to the Totara Island is cut off.

The drilling rigs for hydrocarbon production of Totara Island located in the Senta's EEZ were occupied and now are under the full control of armed men with no State identification.

Response to Vignette 4

Participants agreed that a state of war existed between Senta and Bastan and that martial law would be declared. It was determined that the Navy and the Marines would be required to deal with the situation on Totara Island.

Requests for international support were discussed. Participants felt that territorial incursions by Bastan forces justified an international response by NATO, the UN Security Council and others.

Participants agreed that government cooperation with the telecommunications industry would be required in order to restore GSM service. There was no clearly identified process for coordinating cooperation between the government and the private sector.

Inject 4.1.1: Day 56: March 2, 05:00

Armed men occupy eight gas rigs off Totara Island in the Senta's EZZ without insignia who used helicopters to land on the rigs and took them over.

Response to Inject 4.1.1

Earlier in the scenario, additional security assets were deployed to these locations to include increased maritime security presence, underwater gas pipeline security measures, oil rig sites and the island was secured by additional military resources.

Participants assessed that such an attack from helicopters would have been repulsed and any rigs taken would have been quickly recaptured, unless these forces received significant support from Bastan.

Inject 4.1.2: Day 58: March 4, 02:00

A significant number of heavily armed men without insignia land on Totara Island at night. Reports about the takeover of local institutions and major Senta's naval base on the island. Cargo ships with no state flag identification are used to block access to the naval base completely. Loss of GSM signal on the island and in the Southern region of Senta.

Response to Inject 4.1.2

NA

3.5. Vignette 5: Post-Crisis Stabilisation

The present vignette focuses on post-crisis and recovery stabilisation process. Post-crisis stabilisation takes place after the end of the crisis scenario – from March 7, 20YY. Crisis management issues are to be discussed, as well.

Each syndicate will be presented with several questions for the post-crisis stabilisation discussion.

Post-Crisis Stabilization

1. How do you see the mechanism for improving the system of critical infrastructure protection based on the results of crisis management?

Response

Participants offered the following: enact laws that clearly delineate authorities and roles and responsibilities for protecting and enhancing the resilience of critical infrastructure; establish a clear chain of command to streamline the decision-making process and to ensure unity-of-effort across all levels of government; approve, exercise and update as necessary a suite of CIP plans that are applicable across all levels of government – national, regional and local; and develop CIP-specific training and exercise programs.

2. Do you see a necessity to improve the existing legal framework on CIP?

Response

Participants noted that no legal framework currently exists – each agency has their own decrees and regulations but nothing that unifies across all. There were a few items that group members stated could be done to improve the existing legal framework such as: increase the severity of penalties for attacking CI sites; classify CI based on priority; and to draft a law (National Resilience Concept) for Critical Infrastructure Protection that lays out the duties and responsibilities for CIP. It was further recognized that current plans likely do not align with the draft law for CIP and more work will be needed to ensure a coherent regulations.

3. Is it necessary to create a single state body to coordinate critical infrastructure protection (subordinate to the President/NSDC/Cabinet of Ministers) or to delegate authority to the already existing state bodies?

Response

Participants did agree that such an entity should be developed but also highlighted that only the Cabinet of Ministers has the authorization to create this body and that it must be subordinate to the Cabinet of Ministries.

4. When was the last time that measures/plans ensuring the continuity of the critical infrastructure management function were updated/executed at the national, regional and local level?

Response

Participants discussed that once the Draft law is enacted, plans can be written that align to it and exercised accordingly. However, practices do exist by sectors such as energy, civil society, and counter-terrorism. The concept of "critical infrastructure" is not included in current legal frameworks. Still, the measures identified in sector plans are trained and exercised. There is a plan to consolidate the currently fragmented legal frameworks into one framework regarding critical infrastructure and protection. The concept of national resilience has been recently approved by the president and planning is underway for the development of a comprehensive legal framework on critical infrastructure and protection.

3.6. Key Takeaways

Requirement for a national critical infrastructure (CI) coordination agency. Resilience to hybrid threats/attacks requires situational awareness at national, regional and local levels. The exercise highlighted the need for a national critical infrastructure coordination center to analyze intelligence and share information with national, regional and local decision-makers. **Recommendation:** Establish an interagency national infrastructure coordinating center in regulation at the Cabinet of Minister level to: analyze threats; provide indications and warnings of potential all-hazards threats and risks during both steady-state conditions and in response to crises; and to facilitate the sharing of CI related information to authorities at all levels of government and the private sector as appropriate as there is no current regulatory framework. This governmental agency should be authorized to provide direction and command

instructions to all agencies for approval by the Cabinet of Ministries. The process must be institutionalized. The Commission on Emergency Situations and Technological Security could be transformed to fulfill this role.

Requirement for a standardized critical infrastructure vulnerability assessment methodology. Developing and implementing meaningful CI protection and resilience measures is dependent on identifying relative risk to critical infrastructure systems and assets. While vulnerability assessments are being conducted by sectors, there is a requirement to revise and update them into a centralized process. The exercise highlighted a requirement for the development and implementation of a centralized standardized CI risk assessment methodology. **Recommendation:** Develop a standardized CI risk assessment methodology based on international risk assessment standards (ISO 31000) or other assessment programs currently employed by other nations.

Requirement for a national critical infrastructure taxonomy and database. Implementing plans, policies and procedures to protect critical infrastructure and enhance its resilience requires a clear understanding of CI sectors, systems and assets. The exercise identified a requirement for a national inventory of CI systems and assets. Applying a detailed, structured system to help categorize assets by sectors, sub-sectors, segments, sub-segments, and asset types, minimizes the potential for confusion. **Recommendation:** Develop a standardized, national infrastructure data taxonomy that establishes a detailed and structured terminology that facilitates data discovery, management, and enables data sharing amongst authorities at all levels of government.

Counter Unmanned Aerial Vehicle Capabilities. With the growing threat from drones, participants identified that Ukraine has limited capabilities to effectively defeat these threats. Currently, its limited capabilities to defeat drones exist with the military, but Ukraine lacks up to date technologies to best counter drones. As well, several agencies beyond the military require the technical knowledge and capabilities to defeat these threats. **Recommendation:** Provide appropriate agencies responsible for critical infrastructure protection the technical experience and capabilities to defeat such attacks. Consider pathways towards procuring latest technologies and best practices from international partners.

Risk Assessment System is reactive not preventive. Currently, strategic planning is focused on reactive measures. A proactive strategic planning system that assesses risk and focuses on prevention is lacking. There is neither an organization responsible for this or personnel capable of performing these duties. **Recommendation:** Develop an organization that is responsible for and capable of conducting strategic risk assessments. This responsibility should reside with the to be developed interagency national infrastructure coordinating center.

4. Syndicate 2: Cyber Security

The Cyber Security Syndicate discusses vignette inject responses during the NATO CORE 20 – Black Sea TTX.

4.1. Vignette 1: Pre-conflict Phase: Hybrid Influencing

Political and economic intimidation against Senta by Bastan authorities is growing. On the basis of the gas transit agreement, which has been signed by Bastan and Senta last year, the Bastan government accused Senta of infringing agreement provisions. Senta denies any violations. However, Bastan's media and some Senta's media controlled by Bastan keep spreading the messages about Senta's violation, stressing the importance of the corresponding agreement for Europe's energy security as the gas transit to European countries is partially ensured through the territory of Senta.

The situation is aggravated by the fact that there is no new contract for gas supply between Bastan and Vela. Given disputes over contractual provisions, Bastan temporarily substantially reduces gas supplies to Vela. Vela maximally draws gas from the transit pipeline, limiting gas supplies to Senta's customers in the Odesa region, near the border with Romania.

Meanwhile, Bastan inflicted import restrictions on Senta's agriculture, manufacture, and metal products, as well as fuel, chemicals, and petroleum products. Besides, Bastan ceases to supply oil products to Senta with automotive, railway transport, and pipelines.

Three websites were found on the Internet with identical visual designs and features of the official websites of Senta GTS Operator, PSG Operator, and Naftogaz Company. Moreover, e-mails with phishing features and attached Microsoft Word text documents have been found in the e-mail boxes of Senta's regional government agencies.

Media reports were released about the powerful cyber-attack on Liebherr's internal network in Germany. As a result, port cranes at the Poti Sea Port in Zestan have stopped working.

From the middle of December, Senta's coast guards are regularly reporting about the Bastan's Navy presence in the Senta's EEZ. It is reported that Bastan conducted military exercises in the Noir Sea in the nearest vicinity of the fairway passage of merchant and passenger ships from/to ports in the Odesa region.

Response to Vignette 1

Participants responded to the escalating situation across the three injects in Vignette one with a high degree of technical detail and a substantial amount of debate surrounding high level coordination and required actions for state owned and private companies. The Syndicate members were not overly concerned with the initial Denial of Service (DoS) attacks on the public websites of Senta's central government institutions and the debate focused on which websites were under the protection of the cyber security service and when different levels of government response (e.g., computer emergency response team of Ukraine (CERT-UA)) or Internal Security (SBU)) should be informed and involved in the response.

Inject 1.2.1: Day 11: January 16, 12:00

Public websites of Senta's central governmental institutions (Parliament, Presidential Office, Ministry of Defence, and Ministry of Foreign Affairs) and regional state administrations are not accessible. Experts suspect a DoS (Denial of Service) attack on these resources.

Response to Inject 1.2.1

Responders to this situation would be Internal security (SBU), the State Service of Special Communication and Information Protection for each organization that was under attack (standard procedures within two hours). The divisions responsible for information security of all attacked stakeholders should also be involved. No significant effects and no cascading effects were identified. If it is a part of a major operation then there would be further coordination across the government but early and unsophisticated DoS would not have significant effects The immediate required response would be to Inform CERT-UA and activate the websites' backups (as all are doubled in terms of hardware, with multiple internet providers and IP addresses (including overseas servers to ensure redundancy and availability)). In addition, a communication plan would be activated to ensure the populace has access to accurate information from central government and regional state administrations. The main areas of concern were not technical or procedural but rather had to do with signaling and sharing accurate information to the general populace. There was broad agreement that in a DoS case like this the populace could find out what was happening by first going to the President's website and then the regional state administration's website. The government has set up contingencies in these cases and they have alternative sources of information from verified accounts on Telegram and Facebook.

Discussion comments: Initial conversation revolved around informing the national command authority and national cyber command center. The group identified several important timeline requirements for informing concerned parties (7 days for max time to notify of the attack in writing and one day requirement ISP to manage and secure against DoS attack). The team focused on evaluating how critical the service or website was (which was under DoS) and what effects it's compromise could have. They highlighted that this DoS is easier to handle than more sophisticated attacks.

Inject 1.2.2: Day 14: January 19, 02:00

Suspected cyber-attack spreads to other sectors – access to websites of significant banking systems (PrivatBank, Oschadbank), news agencies and portals is disrupted.

Response to Inject 1.2.2

Each bank individually and the National Bank of Ukraine would coordinate responses on the banking side. Privately owned news agencies would have their own internal cyber security and threat response teams and would also report to the National Police to open criminal investigations. It is likely that a coordinated attack would also involve Internal security (SBU) as an investigator and responder. There was a discussion of website vs. banking system (e.g. apps and transactions) being affected which made a large difference in assessing the effects. If the latter are not affected then there will be no widespread panic - or will it be an indicator for future expected events. Possible panic would ensue if these banks were unable to pay for pensions and be used to purchase services. Increased concerns about the possibility of larger attacks and loss of key information about the events could cause widespread confusion and impact the broader economy and civil society. Some areas of concern which may prevent an effective response are: the taxonomy of incidents and reporting requirements were identified as a problem as there is no definition of cyber crisis and each state owned and private organization has its own procedures and rules. The participants highlighted low levels of trust in law enforcement agencies for private companies resulting in work with contracted security or directly contacting the special communications agency. As there were no participants from outside of large state-owned companies (e.g. the National Bank of Ukraine and NaftoGaz) it was not possible to get the private company perspective on the events. It was also noted that while in the case of the banking system, the National Bank of Ukraine coordinates the actions/communications, each bank might also provide its own response, especially on social media.

Discussion Comments: These escalating attacks cut across private and public organizations with different levels of resources, protection, and response requirements and so there was a lot of discussion in the Syndicate about the responsible parties and their required actions. Outside of reporting to the National Police for the initiation of a criminal investigation or reaching out to private (contracted) security, most companies such as news agencies do not have standardized responses or reporting requirements, which may be required so that there can be effective response by public institutions.

Syndicate members also discussed the need for more robust cyber response centers and staffing at the computer emergency response team of Ukraine (CERT-UA) and in the National Police. While in theory operators and dispatchers are available 24/7 to collect and process information and technical details of attacks and react to the threats in coordination with CERT-UA the reality is that they do not have the capacity. This also creates problems when attempting to determine if the previous and current incidents are connected or coordinated and in determining if they are systematic.

Inject 1.2.3: Day 16: January 21, 11:00

Attacks on utility online billing and payment centres in the Odesa region have been reported. The cyber police regional unit registers complaints from individual citizens that their data on the utility services consumed does not correspond to accurate information and, as a result, there are outstanding debts in the system.

Response to Inject 1.2.3

The syndicate identified the private utility billing agency and computer emergency response team of Ukraine (CERT-UA) as the responders. CERT-UA is not a private company but service centers that are part of the utility concern, for example, the Center for Communal Service in Kiev. The group discussed the nature of the attack - if on the billing system (not the recording and metering system) then effects would be minimized. Possible cascading effects were identified up to and including people protesting in the streets due to perceived debts. The required response in this case would be to have the private billing company work with the National Police to initially investigate the claims of fraudulent bills. This was identified as a continuing attack on the stability of the country, so there would be coordination between the office of the president and the local government. In addition, there would be communication between the cyber security entities, the company leadership, and the media in general with the possible coordination of press conferences and other strategic messaging. The main area of concern was from the standpoint of rapid and accurate technical reporting of the incident to the government from the private company. Private companies are reluctant to connect to the system for cyber incidents and there was no single point of contact identified. In addition, capacity gaps in the cyber police in a situation like this were expected as the existing system would be overwhelmed by large scale events and excessive reporting of billing issues from the public.

Discussion Comments: The attacks on the pension fund payment and processing systems historically resulted in delays and contributed to destabilization in the country, however due to the way that billing is done with gas there are several options to respond quickly (e.g. having the users pay their projected amounts rather than billed amounts). One of the things that helps calm people and stabilize this situation is that there is a ready-backup which is analog and independent of the billing system. Participants noted that press releases were made when this happened once before with pension funds and responses would likely be modelled off of that successful precedent. Syndicate members also highlighted that once a state emergency was issued, the State Emergency Service could cover much of the needed coordination and response but a plan approved by the cabinet of ministers would be required first, to determine how critical the situation is.

Vignette 1 Participant Summary:

Vignette 1 began as a simple denial of service (DoS) attack on government websites and escalated into attacks on the banking systems websites, news outlets, and the bill paying systems of public utilities. Participants noted that in each case the origins of the attacks, their coordination, and severity were all uncertain. The Injects provided a challenge as they cut across private and public organizations with dramatically different levels of resources, protection, and response requirements. This created two sets of challenges that needed to be negotiated by the members of the Syndicate: responsibility for actions and reporting and response coordination.

State owned organizations have to have the resources and staff to respond to events and are well connected with internal security and crisis response at the national and local levels. For example, the National Bank of Ukraine is state-owned and under its own regulations and controls, other banks are publicly owned and under the protection of the international banking security system. If banking systems are unavailable for longer than designated periods then the National Bank of Ukraine is informed and there is a public/national response. At the level of each bank there is a risk manager who is responsible for all risks including cyber. The banks are required to contact CERT-UA within certain timelines depending on the severity of the attack and consequences.

In the private sector responses are more complicated, outside of reporting to the National Police for the initiation of a criminal investigation or reaching out to private (contracted) security, most companies such as news agencies do not have standardized responses or reporting requirements. This highlighted the need for better definitions of reportable events, public-private relationships and messaging. There was broad agreement that in the case of news agencies or billing companies failing the populace could find out what was happening by first going to the President's website and then the regional state administration's website. The government has set up contingencies in these cases and they have alternative sources of information from verified accounts on Telegram and Facebook but they may not be able to gather the initial reports from companies without higher degrees of trust and more established reporting requirements. It was noted that there is no definition of a 'critical' situation, only a set of general categories. This hampered overall government response to a distributed set of attacks, especially in the space of messaging and sensemaking early in the problem.

4.2. Vignette 2: Low-intensity Hybrid Operations

Weather conditions in the Southern regions of Senta deteriorated at the beginning of February. The wind speed reaches 50 m/s index causing considerable damage, namely in the Odesa region.

Bastan's import restrictions on Senta's agriculture, manufacture and metal products, as well as fuel, chemicals and petroleum products contribute to the decline of Senta's economy which has already been in recession. Pro-Bastan activists use the economic downturn as a chance to intensify protests against Senta's government. Social tensions reached their peak when news about Odesa City Council's decision concerning secession of the Odesa region from Senta has spread via the Internet.

The work of Odesa Sea Port is continuously disrupted by the actions of pro-Bastan activists and incidents in the cyber-security domain. Moreover, Senta's civilian and coast guard vessels reported technical issues in their navigating system.

Furthermore, Bastan's vessels act aggressively against Senta's fishing boats. Coast guard ships of Bastan intimidate and threaten cargo vessels of Senta and foreign states as well. Recently, Bastan Naval Forces provided support to the illegal gas exploration and drilling rigs installation operation within the territory of Senta's EEZ. The 24-hour security guard patrol of Bastan's Navy was established around the rigs.

Response to Vignette 2

Participants responded to escalating attacks on numerous government-and-privately owned systems throughout the course of Vignette 2, starting with website defacement and escalating to malicious code on the network of Pivdenny Bank and associated DDoS attacks on the Senta National Bank. Syndicate members drew attention to the challenges associated with complex lines of authority and jurisdiction when the private sector is under possible attack or suffers losses. Elements of the participant's discussion centered on the challenge of realizing what is happening and being able to distinguish between signal (actual cyber attacks and hybrid warfare) vs. noise (environmental factors and natural events) affecting relevant information systems. Participants demonstrated a clear understanding of state capabilities (e.g., SBU and National Bank) but were more uncertain about private companies' capabilities, readiness levels, and cyber-specific requirements levied on private industry. Discussion also highlighted the challenges this poses to coordinated response between state and private entities and for the international community. Numerous participants also brought in relevant historical examples and personal experiences when dealing with challenges such as debunking information operations like the one in this inject.

Inject 2.2.1: Day 24: January 29, 12:00

The website of Odesa City Council states that regional authorities decided to declare independence from Senta and become the Odesa Autonomous Republic.

Response to Inject 2.2.1

The required responders in this case are Internal security (SBU), the Office of the President, Parliament, and National Security and Defence Council. There is potential for serious cascading effects in this scenario as the changes on the website could serve as international provocation and this act could be a first step in activating separatist groups and could result in a coup. The response required would be notification of military forces (if it is real information), the State Service for Special Communication Service and Information Protection and CERT-UA would all be done immediately. Central government would focus on debunking the information, making it public and clear that this was a criminal action. Other branches of government would be notified and information about the nature of the attack would be shared broadly. In addition, a communication plan would be activated to ensure the populace has access to accurate information from central government and regional state administrations. There is concern about the timeline associated with certain parts of the responses and the team thought it was critical to ensure that the website was not turned off intentionally as it could be an indicator of truth of claims. Proper rebuttal and control of the message and the timelines associated would make the difference between the message being viral and destabilizing or being only a small impact. Lines of authority and jurisdiction are complex in this situation with the SBU being the one that decides/determines what is true and if it is cyber then the cyber police getting involved. SBU will process information and report it to the government and the president, they are the landing pad for that information from the National Police which is where citizens will first reach out to.

Discussion Comments: Discussion by participants focused on determining the ground truth after initial responses were taken. The website operations teams would be required to find out what happened and how it happened and then deliver this information to the SBU and national police and also to the Oblast administration, as they are subordinate. The nature of the event (whether it is simply a crime or an attempt at a coup by a nation state actor) will inform the follow-on actions. Members of the Syndicate also debated timelines for determining the truth of the event and best practices for reliable communications with the populace. Historical events in Sevastopol were used as a reference point for debunking information operations like the one in this inject.

Inject 2.2.2: Day 30: February 4, 16:00

A cyber-attack on the Odesa Sea Port website. Administrators lose control over the mail server. The webpage identifying the location of the cargo vessels within port terminals are unavailable. After the website's restoration, a major part of the volume and cargo status information has disappeared.

Response to Inject 2.2.2

Required responders to this scenario would be the sea port is the owner of the website and responsible for the data. The National Police will also investigate the incident and may report it to State Security (SBU). The effects of this scenario are that port operations are compromised and this extends to ships schedules, loading, unloading, and billing. Possible cascading effects international issues, ship owners, cargo owners all implicated in this event including international implications and connections to insurance companies. The required response would be that the sea port and its private security and database teams be responsible for restoring backed up data, communicating the incident to the public, and restoring normal

port operations. The SBU would investigate the nature of the attack and work with National Police to identify the origin of the attack and appropriate state response. Some areas of concern the group noted were: the lack of trust between the sea port and other private industry makes the coordinated response more difficult. The participants highlighted the historical damage to reputation and cooperation challenges sharing data with the National Police has caused. There are currently no requirements for reporting and official designations of critical infrastructure.

Discussion Comments: Syndicate members agreed that Security service of Ukraine (SBU) has a regional administration with divisions of protection of the national interest in ports and that they would be instrumental in the response. The CERT-UA in Kyiv would be the one to provide direction on how to proceed in the cyber domain (if informed by the port and SBU). Back-up copies are required for all databases because it is critical infrastructure (this already exists). It is up to the ministry of infrastructure to determine the required actions and enforce this rule (which the Syndicate members did not believe was rigorously enforced). The state control over the hosting of electronic resources in private-owned objects of critical infrastructure should be reinforced.

Inject 2.2.3: Day 40: February 14, 20:00

Media and social media have information on the public availability of information on utility billing, indicating customers' personal data, such as name, address, telephone number, e-mail.

Response to Inject 2.2.3

For information protection and validation, the billing company is the required responder and as for the criminal investigation and state response the required responders would be local and National Police. The release of this information will lead to mass confusion and complaints. If authentic it could result in mass scams for Ukrainians. If personal data includes the data of EU nationals, then national legislation steps in and there is a potential for GDPR fines. There would have to be a National Police investigation to determine the authenticity and source of the leaks. The service provider (subsidiary to the larger government organization which runs gas) would be the responsible party for any negative effects on Ukrainian citizens and foreign nationals. High level national engagement may be required depending on the medium of dissemination of the personally identifiable information (PII). CERT-UA and the Council of National Security and Protection would be involved. An area of concern the group noted were the absence of a dedicated team for the removal of criminal content on the internet for cases like this (currently internal affairs handles such issues). DoD members of the Syndicate brought up concerns regarding the authorities to take down the source of the PII but in general the response from the group was that there is no mechanism for leaks in social media messengers. Using software (automated monitoring) solutions and cyber risk insurance would need to be mandated to ensure risk mitigation but currently are not. International standards to define the cyber readiness level and cyber response plans would also aid in an effective response.

Discussion Comments: Syndicate members were reluctant to jump to conclusions and connect this event to the rest of the vignette as it is unclear if the data is actually authentic and if the data was leaked by a disgruntled employee or as part of some larger operations. Capabilities in the government and/or strategic partnerships with social media companies for options to take down or deny access to PII on the internet was part of an in depth discussion by the participants but did not arrive at any conclusions.

Inject 2.2.4: Day 43: February 17, 10:00

A tanker belonging to Senta suddenly loses control and collides into Bastan's cargo ship in Senta's EEZ, causing a significant oil spill over. Bastan accuses Senta of sabotage.

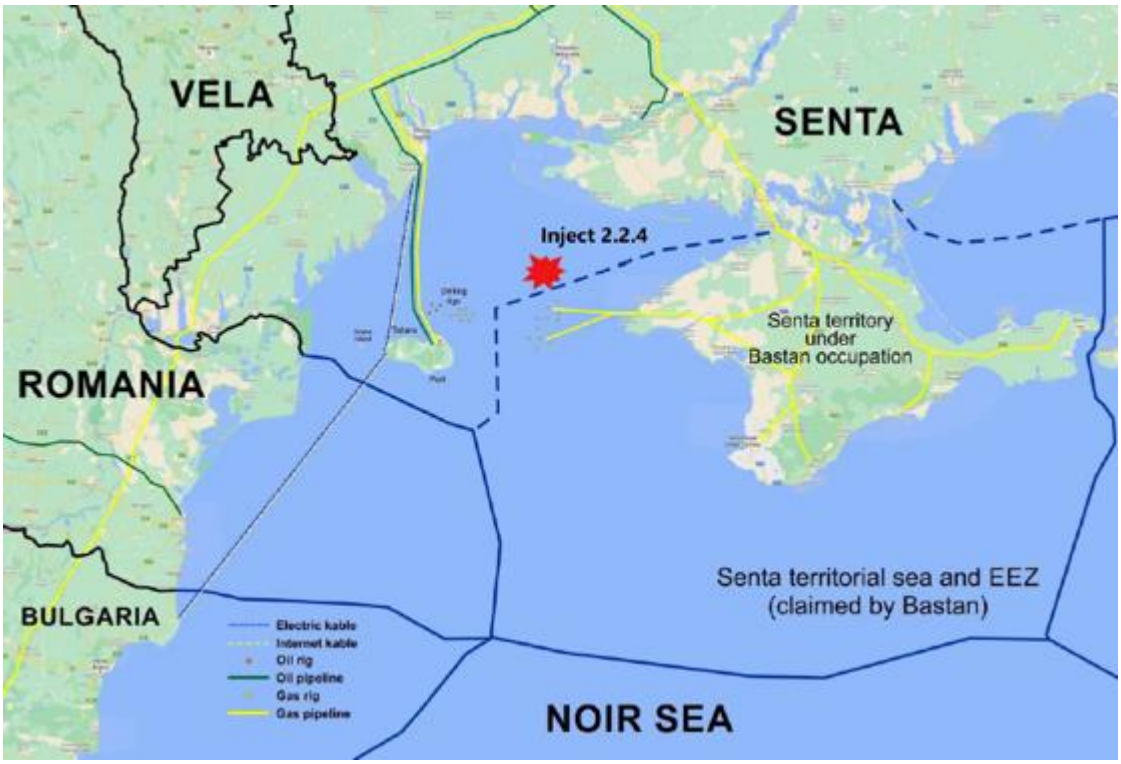
Response to Inject 2.2.4

Required responders in this situation would be Maritime Administration coordination (commercial and not Navy), National Ministries and General Staff of Armed Forces of Ukraine, SBU, and international partners. This event could have major economic and international consequences. The response would require coordination of investigation and messaging at the national level (National Security and Defense Council of Ukraine, SBU, National Police, General Staff of Armed Forces of Ukraine, Intelligence, Ministry of Internal Affairs, and Ministry of Digital Transformation). Evidence collection and records would need to be obtained by the State Service of Special Communication and Information Protection. The National Cyber Security Coordination Center can reach out to track down the interfering signals or evidence. An area of concern is that there is no protocol for what is necessary but an event like this would be driven by larger geo-political requirements and be coordinated at the national level.

Discussion Comments: Syndicate members were unsure if there was a cyber element to this event. They provided ideas on how to confirm one way or another that further cyber syndicate involvement would be required.

Inject 2.2.5: Day 46: February 20, 10:00

A malicious code is detected on the network of Pivdenny Bank. A DDoS attack is carried out on the ITS of the Senta National Bank State Office in the Odesa region.



Response to Inject 2.2.5

The first response in this situation would be from the local bank (Pivdenny Bank is incorporated in the Odessa region). The national bank of Ukraine regulates cyber security for the whole banking system. This

event could have major economic and international consequences including a mass panic and a loss of confidence in the banking system by the Ukrainian people. The expected response would be that the bank starts the incident management procedures and the commercial bank will inform the national bank on the incident. There is a special platform (over 60 banks connected) to share incident response information (filling in specific forms). NBU provides recommendations in terms of responses and information is shared with CERT-UA for follow-on forensics. The participants noted that there are no standard responses for this issue - there are requirements but not clear instructions and procedures for this situation. Site will be investigated and if necessary international experts will be called on. The scale of the situation needs to be assessed to determine if it is an act of war.

Discussion Comments: Syndicate members mentioned that the bank is categorized as critical infrastructure so any incidents need to comply with emergency management. NBU representatives are confident that a DDoS attack will not be effective (and they have special services that they have bought to help them handle it).

Vignette 2 Participant Summary:

The escalating severity of cyber attacks in Vignette 2 highlighted the difference between state and private organizations in terms of their capabilities, coordination, and cyber response. Syndicate members agreed that the Security service of Ukraine (SBU) has a regional administration with divisions of protection of the national interest in many critical national industries (including ports) and that they would be instrumental in the most responses.

For the commercial banking system, incident management procedures were well established and generally involved the commercial bank informing the NBU on the incident in question. There is a special platform (over 60 banks connected) to share incident response information (filling in specific forms). NBU provides recommendations in terms of responses and information is shared with CERT-UA for follow-on forensics.

For private industry, there were two key takeaways. First, the lack of trust between private industry and elements of law enforcement makes the coordinated response more difficult. The participants highlighted the historical damage to reputation and cooperation challenges sharing data with the National Police has caused. The second is that there are currently no requirements for reporting and official designations of critical infrastructure. For example, in the case of the port database attack, back-up copies are required for all databases, however Syndicate members did not believe it was rigorously enforced.

4.3. Vignette 3: Conflict Phase: High-intensity Hybrid Operations

Senta's critical infrastructure experiences a wide range of kinetic and non-kinetic attacks. Disruptions occur on the natural gas transmission pipeline in the Southern gas transit corridor, affecting supply to the Southern region of Senta and the neighbouring foreign states. Moreover, there is a threat of disruption of the heating season not only in the southern part of Senta but in Kharkiv and Luhansk regions as well, in particular those heavily depending on the gas supplies from Bastan.

In the South of Senta, there is a one-third increase of the number of emergencies, fires and accidents caused by arson and terrorist attacks using explosives, which in turn has led to a significant increase in the number of casualties. A significant incident is suspected in PJSC 'Odesa Portside Plant' where the considerable release of hazardous chemicals is reported.

Information on disruptions in the South Senta NPP operation is disseminated. Bastan's media blames Senta's authorities for the release of radiation. Almost at the same time, information about the attack against hydroelectric pumped storage power plant attack is being spread.

Massive cyber-attacks disrupt the operation of the Odesa Sea Port, including transportation and cargo handling. The branches of Oshchadbank and PrivatBank banking systems in the Odesa region were attacked.

In a month after the first cyber-attack on Liebherr's internal network in Germany, there have been a series of minor cyber-attacks on the Liebherr's port cranes all over Europe.

In the maritime domain, Bastan's Navy ships are increasing their presence in the Senta's EEZ, using navy exercises and interrupting the international passenger and cargo sea transhipment.

Response to Vignette 3

Syndicate members had a robust discussion surrounding the introduction of more complex problems such as advanced cyber attacks, bad signals off of equipment, and finally large scale mass casualties as a result of cyber-hybrid operations. They also highlighted the fact that there are cyber teams and monitoring teams always on site and looking at the operations of this very expensive equipment - but they are likely to look at these problems in a technical rather than cyber light. This ambiguity and the length of time required to verify a cyber attack properly remained central to the discussion.

Participants also relied heavily on the SBU as a central clearing house for information and response to cyber threats, although this may be the responsibility of both the the State Service of Special Communication and Information Protection and the cyber police. The participants pointed to a strong bias towards the role of the SBU, which was formed due to the loose observance of the law. They also stated that the SBU independently carries out investigations and decides who to inform in these different events and that it was likely that there would be enhanced measures for protection due to increased threat level. Such an approach introduces an imbalance in the powers of the State Service of Special Communication and Information Protection, cyberpolice. Exercises done by the SBU may or may not include cyber testing.

Inject 3.2.1: Day 52: February 26, 12:00

Suddenly the automated systems of the workflow of the operators of the Odesa ports fail. All information about cargo storage and handling at ports is lost. Similar incidents are reported in the energy and banking sectors – no online banking services are available.

Response to Inject 3.2.1

The responders in this case should be the National Cyber Security Coordination Center (NCCS) and SBU, in coordination with the NBU and local agencies will be the first responders. NBU will determine if a crisis exists and can enact emergency measures in the banking system. National level response will be coordinated as required by the Minister of Internal Affairs. The three domains are all critical. The three domains that are under attack are all interrelated. The blackouts will probably be the first and most obvious effects followed by the economic damage. The electrical blackouts will dominate the problem due to the cascading effects bringing everything down (such as water, transport, etc.). Other cascade effects could be international regarding cargo. SBU will likely be lead since they are in charge of counter-terror operations. SBU will inform NCCS. NCCS will determine the membership in the team and coordinate each

domain's cyber center's responses. In addition, each organization reports to CERT-UA with the possible exception of the seaport which does not have officers who have this responsibility. An area of concern is communication from DoS to National Police due to high number of claims from multiple sources. Without clear definitions of reportable problems, it will be a challenge for higher level echelons to ensure they have good situational awareness. The procedures that they refer to are not actually written, disseminated, and practiced by the teams here e.g., participants agree that something like 5 banks under attack is the threshold for reporting to the National Security and Defence Council but there is no established tripwire. Representatives from the energy and port sectors were not present.

Discussion Comments: Syndicate members highlighted the fact that State Service of Special Communication and Information Protection is not represented in the port administration (but there are non-classified channels of communication). The team believes that the backup information and processes will keep the port working. The port has employed some cyber security experts but is not connected to NCCS. There was also discussion around certain procedures that should be approved regarding who will report to the media (NCCS may or may not) and the role of software providers in providing rapid forensics and solutions if certain information is provided.

Inject 3.2.2: Day 53: February 27, 04:00

A cyber-attack is suspected at several compressor stations (CS) of the Southern transit corridor: Berezivka (Odesa region), Pavlohrad (Dnipro region) and Marivka (Mykolaiv region) - as some remotely controlled valves malfunction and operators see wrong readings from sensors. The flow of transit gas on the South-Eastern part of the Odesa region is interrupted.

Response to Inject 3.2.2

CERT-UA was determined to be the first responder. SBU is informed and decided on further activities as they own the locations because they are part of counter-terror infrastructure.

Effects: The gas flow during a critical cold time is disrupted. Extent of attack and other affected areas is unclear. Potential need for emergency response in the cold.

Required Response: SBU is lead on this and has procedures including investigation into the sources of the attack. They believe that the compressor station can be recovered and readings taken manually. Forensic teams are deployed to determine if there is a cyber element to the attacks. CERT-UA is the platform to collect all the information.

Areas Concern (which prevent effective response): Realism/feasibility of the scenario given the specifics of how meters are hard-wired (analog). There are not clear reporting lines. SBU reports to the office of the President and it is unclear if information is disseminated to other people afterwards. Final agreement about CERT-UA being the collection platform (but only after long conversation). Sharing requirements for Indications of Compromise (IOC) are not properly determined.

Comments: The Syndicate members debated the realism of the scenario given the technical details (e.g., how much remote control of the valves is actually possible) and noted that historically they have been able to identify cyber-attacks on the gas system and harden it against adversaries. They also stated that the SBU independently carries out investigations and decides who to inform in these different events and that it was likely that there would be enhanced measures for protection due to increased threat level. Exercises done by the SBU may or may not include cyber testing. Main problem of SBU functioning and response to

this inject is that SBU during the implementation of measures to prevent terrorist activities frequently doesn't consider cyber component in such kind of attacks. Also State Cyber Protection Center of Ukraine on a regular basis takes measures to test critical infrastructure networks for vulnerabilities. In conclusions I recommend that this two activities (measures to prevent terrorist activities and pentest (penetration test)) should be implemented jointly during the investigation.

Inject 3.2.3: Day 53: February 27, 09:00

Liebherr port cranes at the port of Pivdennyi do not work (system of cranes management failed), inability to organize loading and unloading operations, the perspective of penalties.

Response to Inject 3.2.3

The responders should be the technical support teams locally at the port and in Germany (but might not be available). It is likely that the port will try to take care of things themselves and not report things up. The technical team at the port will be the first responder. The disruption to port operations is crippling economically and major financial losses. Follow-on international and insurance implications are also possible. An important response is to inform other port facilities with the indicators of such threats. Contact support teams and provide them information. If the attack is cyber, inform SCIP/CERT-UA, inform economic ministries and security services of the port. Liebherr may be contacted at the national level if required. A concern of the participants is that the security services of each port do not have a chain of reporting. If there was a chain they could inform NCCS but currently there are no established procedures for situations like this. In the end there are limits to what can be done by local cyber teams - so strategic communications are very important while a solution is found in Germany.

Discussion Comments: The participants discussed the timeframe and methods of establishing a cyber-attack as the cause and appropriate responses given the foreign ownership of the equipment. They also highlighted the fact that there are cyber teams and monitoring teams always on site and looking at the operations of this very expensive equipment - but they are likely to look at these problems in a technical rather than cyber light. One challenge with this scenario is that it is an attack against a technical system that has proprietary software (Liebherr).

Inject 3.2.4: Day 54: February 28, 14:00

Ukrenergo loses control over the high voltage grid SCADA system after an update of the system. Critical substations in the Odesa region, such as 750kV Prymorska, 330kV Novoodeska, Trykhaty, Adzhalyk, are disconnected from the grid. An attack wipes out data in essential system files, causing computers to crash.

Response to Inject 3.2.4

The state-owned company (Ukerenergo) has a highly qualified response team and will respond to this situation. In this situation CERT.UA will provide the general recommendations. There are huge effects on the country from hospitals to streetlights. All systems like water are disabled. There would be turmoil in the streets. International concerns also exist due to electricity export to Vela. Bastan occupation troops may use this as an excuse to occupy. One way to respond would be by managing the whole event internally - automatically upload IOC to MISP and roll back to the previous stable version of software. Ukerenergo will inform other locations/industries/departments. Deployment of cyber forensics teams (from CERT.UA) to determine details of the attack. If there are signs of crime then SBU comes into the picture. Government should provide information and aid in critically affected civilian areas. The group is concerned about the lack of an adequate number of experts trained to respond to the situation was a factor identified by Syndicate members. Officers who deal with the protection of critical infrastructure need to be trained and

employed in peacetime to deploy properly in crisis. The military response team needs to cooperate with State Service for Special Communications and Information Protection (SSSCIP) on a regular basis so that a change between war and peace will not be discontinuous.

Discussion Comments: Syndicate members focused on the possible deployment of military personnel to address these problems and their required preparation, training, and integration with the civilian sector. Also, participants discussed the need for state of emergency and martial law with corresponding distribution of duties between Ministry of Defense and SSSCIP regarding cyber protection of critical infrastructure. The team also explored the follow-on effects in detail, noting that it is likely that Odessa will not have water or electricity.

Inject 3.2.5: Day 55: March 1, 00:00

After an update of several Programme Logic Controllers (PLC) at Dnistrovska hydroelectric pumped storage power plant, communication of industrial operations is unstable. Unrealistic readings are provided to the operator on power generation values. Besides, suddenly all gates rise to maximum height, causing an uncontrolled and unscheduled outflow of water. This sudden outflow damages the turbines at the hydroelectric power plant, as well as causes rapid and massive flooding downriver.

Response to Inject 3.2.5

The role of State Emergency Service is determined according to the law. In the end the National Security and Defense Council (NSDC) would coordinate a national level response to the event. There will be casualties from mass flooding. Long term consequences, economic damage, international issues (due to power export) and impacts to military readiness and long-term civilian populations and industry. The National Cyber Security Coordination Center will be informed of all events. The decision will be made to call on the national council for security and defense to plan and execute a national level response. Members of the Syndicate highlighted the lack of proper response and cyber protection. The adverse impact on integrated air defense in the region was also brought up. Possible national level (NSDC) command exercises to include private, public, and armed forces collaborating which will be planned by the end of this year.

Discussion Comments: There are questions about whether this is a cyber-attack or an act of military aggression which the participants brought up and the team also focused on discussion of deploying armed forces to help with disaster relief in the aftermath of the catastrophe. Syndicate members discussed the possibility for martial law in the regions concerned.

Vignette 3 Participant Summary:

This Vignette stressed the Syndicate members in asset management, vulnerability assessment, and mitigation/remediation at local, country-wide, and international levels. Sharing requirements for Indications of Compromise (IOC) are fully determined and there are 4 MISPs but there is no single reporting line and set of requirements (participants suggested: National Police > Cyber in National Police > NCCS > SBU > National Council of Defense and Security (RNBO) > President). Procedures for dissemination back down and laterally need to also be established. Determination of cyberattacks remained a challenge - specifically the timeline for investigating cyber-attacks is on the order of weeks to months, and device failures are treated as physical failures until all non-cyber potential causes are ruled out.

The conversation in the syndicate was more about the independent software expertise, the practice of software expertise in the SBU was recognized by members of the syndicate as vicious, because it allowed the counter-intelligence agency to deal with business issues, giving these SBU more powers than provided by law. Pre-production testing requirements were also identified as an area where more work needed to be done by the government. Involvement of the armed forces - soon to be required to do more for protection of critical infrastructure and possible national level (NSDC) table-top exercises to include private, public, and armed forces collaborating by the end of this year were all brought up as next steps.

4.4. Vignette 4: Hybrid Warfare

Tensions between Bastan and Senta have reached the highest level ever. Senta's military intelligence reported an unprecedented number of military build-up in Bastan Navy's bases in the Noir Sea. A significant number of provocative accidents have started to occur on Totara Island. Reports of the loss of GPS and GSM signals on the island. The Internet connection on the island was disrupted.

At the same time, Senta continues to experience a growing number of cyber-attacks against governmental and local institutions, and critical service providers. Bastan's and Senta's media aggressively reports about the inability of Senta's central and local authorities to provide critical services for the population. Moreover, top commanders of Senta's armed forces in Kyiv and Navy officials in Odesa and Totara Island received e-mails from unconfirmed accounts with a direct warning 'not to follow orders of Senta's political authorities, or they and their families will be in danger'.

Social media is full of reports and active discussions about the possible separation of the South part of Senta. The same news is being spread via official web pages of regional councils. The above leads to pressure and tensions inside governmental institutions, law enforcement agencies, and armed forces. In the last 24 hours, street manifestations against the Senta government intensified dramatically, namely in the central cities of southern regions: Odesa, Mykolaiv and Kherson. As a result, the government is overstretched, and the population is confused.

Against the background of significant cyber disruptions, psychological pressure, the spread of misinformation, and growing street manifestations in southern regions, suddenly a considerable number of military forces without insignia launched on the Totara Island. The access to the Port of Totara Island is

blocked by the cargo ships with no State flag identification. The access by water to the Totara Island is cut off.

Drilling rigs for hydrocarbon production of Totara Island located in the Senta's EEZ were occupied and now are under the full control of armed men with no State identification.

Response to Vignette 4

This Vignette raised significant cyber-attacks, electronic warfare, and the invocation of martial law. It also presented challenges for the assessment team due to a lack of familiarity with government actions during hybrid attack - something the participants were much more familiar with. Explanations of specific procedures and provisions under martial law applied by the military were described as events such as those in Inject 1 had happened historically. In that case, Odessa/Oblast council did not follow the military's orders and there was detailed discussion about what to do with local administrations who do not follow orders. The team also differentiated between local and national levels of martial law.

Inject 4.2.1: Day 56: March 2, 10:00

A significant cyber-attack is suspected against major Internet providers of Senta. Internet connection on Totara Island is completely disrupted.

Response to Inject 4.2.1

The primary responder will be the military (due to martial law) and support from State Service of Special Communication and Information Protection. The immediate effects are that the internet connection on Totara Island is completely disrupted which results in panic, confusion, and disruption of economic and civilian operations as well as initially potentially disrupting some military communications. The response should fall on the State Service of Special Communication and Information Protection which has the resources to provide other forms of communication to the island. The military can also provide other forms of communication to the island. The military will receive instructions from the military administration and will direct local civil and military assets to solve the problem. Goal of having information disseminated in one hour to all agencies. Important questions include, has this ever been practiced or done? How important are internet comms on this island? Military will provide hard copies if comms are cut (but unclear how this is coordinated at scale). Adding provisions to the draft cyber security law for determining how the local military command will report to and coordinate with the national level government.

Discussion Comments: The operating assumption is that the internet connection is actually compromised as in the scenario description and that there is martial law in the Odessa region. Participants noted that the State Service of Special Communication and Information Protection has the resources to provide other forms of communication to the island.

Inject 4.2.2: Day 58: March 4, 16:00

Navigation systems were damaged at the ship-boat structure of the Odesa Maritime Guard Detachment of the Regional Maritime Security Directorate of the Senta State Border Guard Service.

Response to Inject 4.2.2

The first responder would be the State Service of Special Communication and Information Protection - as this is presumed to be a case of electronic warfare. Some immediate effects seen are economic and international reputational damage, and confusion. An important first step would be to locate and neutralize jammer/spoofer.

There is a concern that there are no procedures on how to prevent jamming and spoofing of GPS/AIS signals. Nationally there are no procedures to deal with the information getting out to the international network.

Discussion Comments: This is a follow-on from the vessel collision (possibly). After the previous incident they were supposed to have a more robust prevention plan in cases like this. No one in this syndicate is an expert in maritime security, especially in GPS issues.

Inject 4.2.3: Day 59: March 5, 10:00

Totara Island loses GPS and GSM signals. At the same time, the website of the Totara parliament declares that in order to protect the local population from genocide by Senta far-right groups, the island's authorities decide to declare secession from Senta and appeals to Bastan for help.

Response to Inject 4.2.3

The Military administration and SBU (suggestion of martial law) should be the responders to this situation. The aerospace agency can also be involved to investigate the GPS issue. The state control division of the

state service of special communication and information protection. Immediate effects of the situation include confusion and chaos on the mainland, potential violence, confrontations, and riots. Switching to warfare and martial law in specific regions. An announcement to the public that the information is fake after investigation by SBU should be made. There were steps after 2014 and there are very clear procedures on the steps that will be taken in the case of territorial issues like this one. Private industry needs to troubleshoot and re-establish GSM. The location of the island is such that operations can be performed from positions of strength meaning that secession is much less likely. More training and exercises are needed to deal with potential secession(s). It is unclear who will be the key personnel to re-establish the GSM network. There are no clear instructions as to how to divide control.

Discussion Comments: Syndicate members brought up concerns that there might be sabotage of the cell network as there was during conflict in the Donbass. Regular citizens would likely not have access to information - on the mainland citizens might be aware of what is happening but on the island they might not be. In the regions that have martial law cell phone communication is now allowed to be used by military personnel.

4.5. Vignette 5: Post-Crisis Stablisation

The present vignette focuses on the post-crisis and recovery stabilisation process. The post-crisis stabilisation takes place after the end of the crisis scenario – from March 7, 20YY. Crisis management issues are to be discussed, as well.

Each syndicate will be presented with several questions for the post-crisis stabilisation discussion.

Please discuss and answer the following questions:

1. How do you see the concept of updating / working out cybersecurity measures and plans for the existing system?

Response

The main step discussed was the concept of national resilience. This legislation has been written and is waiting for approval by the president. It would enable the Ukrainian government to launch a legal mechanism to build up resilience measures (including cyber resilience) systematically. The lack of an approved list of CI objects has been a challenge to developing plans and the resolution of a cabinet of ministers requires determination of CI facilities but people have not complied yet. Another challenge identified by participants is that Ministries have few experts to focus on the issues.

Additionally, there is no national plan of cyber response. All participants of the discussion agreed that there is a strong need to introduce CISO positions in government agencies, state owned, and private organizations. General criminal law allows for a wide range of responsibilities, so a cyber specific law is required for CI given its importance.

2. Is legislation in the field of cybersecurity provision and development comprehensive (sufficient) enough to date? If not, what are the priority areas for improving it in the post-crisis analysis?

Response

At the state level there is no practice of assessing risk in the cyber domain. Public-Private Partnerships are a priority while also using social network channels for reliable communications to the population – e.g., provide videos and explain things in 'simple words' and look at cases in a way that can be shared with the population at large as the population needs timely information and transparency.

The authorities of Armed Forces, State Service of Special Communication and Information Protection, and private industry at different stages of crisis must be more clearly defined.

3. Today, leading cybersecurity companies and professionals are focused on creating multi-level integrated security systems, the basic principle of which is the proactive management of cyber risks, taking into account the strategic objectives of the organisation (object of protection) on the one hand, and changes in the spectrum of cyber threats on the other. How should cybersecurity compliance be integrated into the critical infrastructure strategy (activities)?

Response

Participants focused on legislation of cybersecurity. Priorities include the identification of level of cyber threat, and carrying out audits of cyber protection including CI. There were a number of data sources and challenges identified, such as:

- Data of SSSCIP
- Data from independent audits (problematic because no independent audits/no mechanisms for this at the current time)

Notable is that SSSCIP found a way out using the "Oxford Model" in place of legislation: Cybersecurity Capacity Maturity Model for Nations (CMM). Link: https://gcscc.web.ox.ac.uk/cmm-dimensions-and-factors#/ . In the private sector businesses should carry out their own audits but the government should provide instructions and requirements and guidance (best practices).

4.6. Key Takeaways

When local or national military control was invoked and participants were uncertain about their agency's responsibilities. Questions such as how the military would employ the civil and civilian cyber resources (e.g., all non-military assets) in the case of martial law were not fully addressed. In addition, the coordination between military and civilian resources was unclear - participants noted that under martial law the state can obtain any communication resources in the interest of national security but there are questions about how private operators are going to cooperate under these conditions.

Additionally, Syndicate members brought up the topic of having a cyber reserve. Currently there are procedures in place which outline the expected number of cyber reserve responders for various situations, however, in order to enlist members as a cyber soldier they need to have a position officially approved and sanctioned by the government - something that has not been accomplished.

Requirement for Independent Assessment of Asset Management. The Cybersecurity Strategy of Ukraine approved by Decree of the President of Ukraine No. 96 dated March 15, 2016, initiated efforts to establish and develop a national cybersecurity system, however, at this time, every agency builds their own structure since there is no unifying legislation. Lacking legislation, national level efforts are hindered and duplicated in multiple agencies. No independent assessment of asset management, vulnerability assessment, and mitigation/remediation have been successfully performed to date. **Recommendation**: The National Center for Cyber Security (NCCS) and the computer emergency response team of Ukraine (CERT-UA) either formally develop a cybersecurity framework or adopt an existing framework in order to perform assessment management, build vulnerability assessments, and create mitigation techniques to improve resiliency.

Requirement for Centralization of the four Malware Information Sharing Platforms. There are four Malware Information Sharing Platforms (MISPs) that are not interoperable or interconnected operated by different government and intelligence agencies. In addition, there are no standard Indication of Compromise (IOC) of attacks across the whole of government in Ukraine. **Recommendation:** Centralization of the four Malware Information Sharing Platforms (MISPs) would increase interoperability and interconnectivity between government/intelligence agencies. Additionally, we recommend standardization of the Indicators of Compromise (IOCs) across the government and international partners.

Requirement to Create National Cyber Reserves. During multiple crisis vignettes, local or national military control was invoked and participants were uncertain about their agency's responsibilities. Questions such as how the military would employ the civil and civilian cyber resources (e.g., all non-military assets) in the case of martial law were not fully addressed. Major capabilities in other state-owned enterprises and companies had not been fully assessed or mapped into response plans. **Recommendation:** Create National Cyber Reserves. The country lacks the concepts of a cyber force reserve and given the specifics of the

training this needs to be determined during peacetime (and go through advanced training in military scenarios). This will also ensure that soldiers are drafted to special units where their skills can be put to the best use and will allow for robust public private partnerships (PPP) for training during peacetime.

Requirement to Implement Digital Evidence Management. Forensic collection of digital crime evidence is lacking in several facets at ISPs. When a digital crime has occurred, a series of data collection events (called a chain of custody collection) similar to that preceding a civil or criminal prosecution have to take place but are not currently occurring. The most notable of these is specifically a consistent method of collecting and storing forensic evidence from ISPs. Also, there is no legal norm for the minimum timeframe that ISPs store data that transits through their network. Currently the data collection processes similar to the civil or criminal process are not consistent between law enforcement agencies and ISPs. Digital collection of evidence, inspection of digital evidence and the forensic determination of the attacker(s), (whether a person or automated attack system) are not currently systematically captured. Ukraine ratified the Budapest Convention (by Verkhovna Rada - the parliament) while did not implement Convention provisions to the full extent. Article 20 of the Budapest Convention is there should a national secondary legal act should be ratified. Along those lines, no unified legal norm for the collection of forensic data/evidence from data providers exists. **Recommendation:** A standardized method (how and what) for the collection and storage of digital data by ISPs (along with law enforcement agencies) to be developed by the Cabinet of Ministers. It should regulate what kind of data should be collected and the way how it should be stored. To provide training for law enforcement personnel along with all personnel engaged in the proceedings regarding the specifics of digital evidence (admissibility, content) in order to bring the digital criminal proceeding to fruition. The legislation on collection of digital evidence needs to be implemented in the near future to support consistent data collection for ISPs. The minimum framework of ninety days should be established for ISPs to store and keep session data, since this data carries critical information of a suspected attacker(s).

5. Syndicate 3: Maritime Security

5.1. Vignette 1: Pre-conflict Phase: Hybrid Influencing

Political and economic intimidation against Senta by Bastan authorities is growing. On the basis of the gas transit agreement, which has been signed by Bastan and Senta last year, the Bastan government accused Senta of infringing agreement provisions. Senta denies any violations. However, Bastan's media and some Senta's media controlled by Bastan keep spreading the messages about Senta's violation, stressing the importance of the corresponding agreement for Europe's energy security as the gas transit to European countries is partially ensured through the territory of Senta.

The situation is aggravated by the fact that there is no new contract for gas supply between Bastan and Vela. Given disputes over contractual provisions, Bastan temporarily substantially reduces gas supplies to Vela. Vela maximally draws gas from the transit pipeline, limiting gas supplies to Senta's customers in the Odesa region, near the border with Romania.

Meanwhile, Bastan inflicted import restrictions on Senta's agriculture, manufacture, and metal products, as well as fuel, chemicals, and petroleum products. Besides, Bastan ceases to supply oil products to Senta with automotive, railway transport, and pipelines.

Three websites were found on the Internet with identical visual designs and features of the official websites of Senta GTS Operator, PSG Operator, and Naftogaz Company. Moreover, e-mails with phishing features and attached Microsoft Word text documents have been found in the e-mail boxes of Senta's regional government agencies.

Media reports were released about the powerful cyber-attack on Liebherr's internal network in Germany. As a result, port cranes at the Poti Sea Port in Zestan have stopped working.

From the middle of December, Senta's coast guards are regularly reporting about the Bastan's Navy presence in the Senta's EEZ. It is reported that Bastan conducted military exercises in the Noir Sea in the nearest vicinity of the fairway passage of merchant and passenger ships from/to ports in the Odesa region.

Response to Vignette 1

Participants debated if Bastan's Navy operations within Senta's EEZ was in violation of (an unknown) national law and/or international law. While participants agreed the Border Guard is responsible for developing and executing a response plan (including requesting) additional forces, the syndicate did not discuss the military capabilities and capacity of Bastan's Navy ships relative to the capabilities and capacity of the Border Guard. In an effort to prevent additional aggression by the Bastan Navy, participants concurred to assign additional forces to ensure protection of critical infrastructure.

A coordination meeting led by the Anti-Terrorist Center would facilitate tasking of the National Guard, National Police and associated domestic security services to establish a yellow threat level for the impacted regions.

In response to the discovery of the explosive device, participants agreed the Border Guard would transit ships/boats away from the Odesa Maritime Security Detachment during the investigation.

Most notably, participants agreed a decision by political leadership would be required to address the attempt by the Bastan Navy to stop the tanker. Furthermore, political leadership would decide if the Senta State Border Guard Sea Service (or alternate service) should be tasked to escort commercial ships arriving/departing from Senta ports.

While not directly addressed by the participants, Bastan Navy activities were labeled by the following terms throughout the vignette: 'provocative', 'violations', 'violations of freedom of navigation', 'obstruction of navigation' and 'aggressive'. The participants did not articulately address what departments/agencies are responsible for addressing each term in accordance with Senta national law and differentiating the definition (for example) of a 'provocation' versus an 'aggressive action'. Participants identified problems with the definition of certain terms in the national law, such as "provocations", "aggressive actions".

Inject 1.3.1: Day 5: January 10, 10:00

Presence of Bastan's Navy in Senta's EEZ has significantly increased in recent weeks. Some navy ships are maneuvering in the contiguous zone of Senta and do not answer identification and information requests by Senta's coastal guards.

Response to Inject 1.3.1

Participants debated if Bastan's Navy operations within Senta's EEZ was in violation of (an unknown) national law and/or international law. While participants agreed the Border Guard is responsible for developing and executing a response plan (including requesting) additional forces, the syndicate did not discuss/debate the military capabilities and capacity of Bastan's Navy ships relative to the capabilities and capacity of the Border Guard. In an effort to prevent additional aggression by the Bastan Navy, participants concurred to assign additional forces to ensure protection of critical infrastructure.

Inject 1.3.2: Day 11: January 16, 08:00

An explosive device is discovered at the parking lot of the ship-boat structure of the Odesa Maritime Security Detachment. Duty service of the Senta State Border Guard Service launches an investigation.

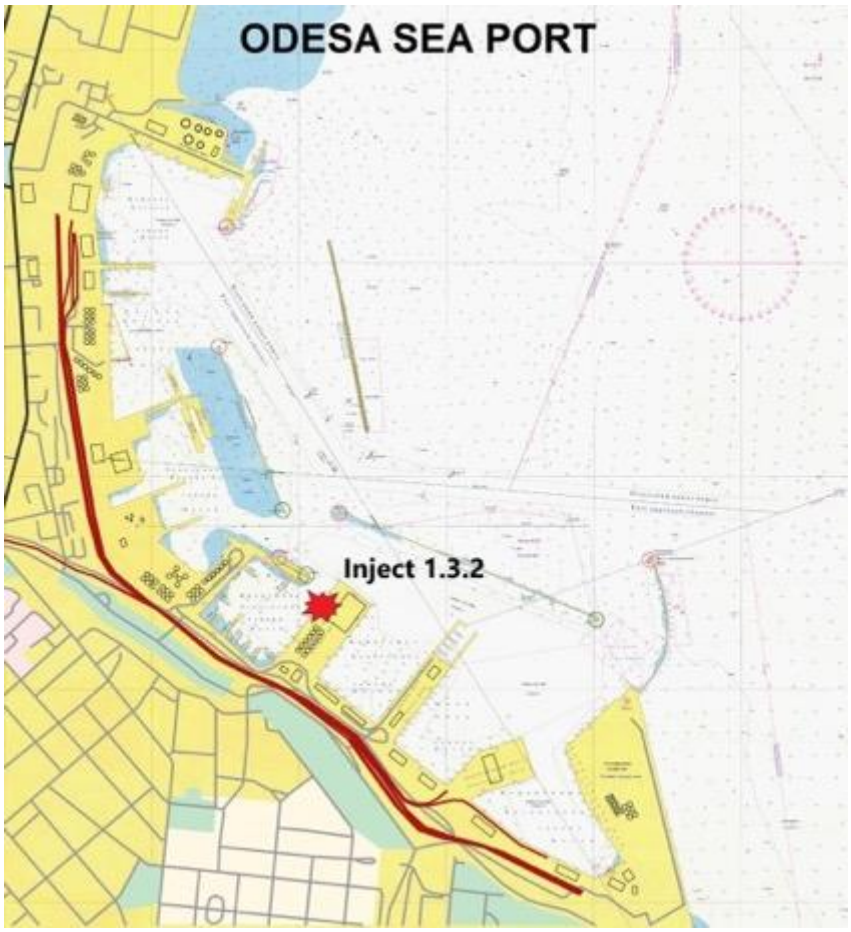
Response to Inject 1.3.2

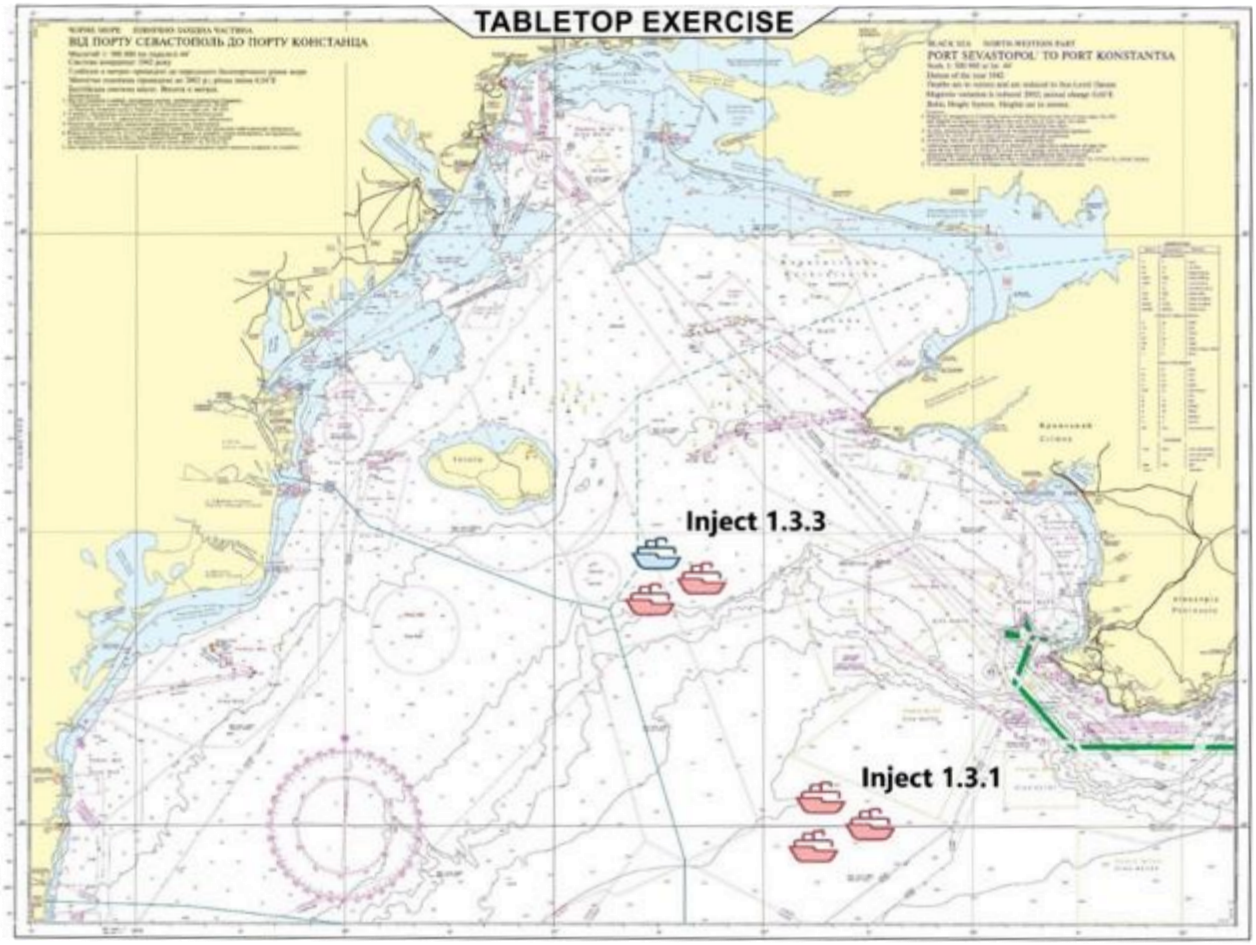
A coordination meeting led by the Anti-Terrorist Center would facilitate tasking of the National Guard, National Police and associated domestic security services to establish a yellow threat level for the impacted regions.

In response to the discovery of the explosive device, participants agreed the Border Guard would transit ships/boats away from the Odesa Maritime Security Detachment during the investigation.

Inject 1.3.3: Day 19: January 24, 12:00

A group of Bastan's Navy ships attempt to stop a tanker moving under the flag of Senta to the Odesa Sea Port under the pretext of "conducting a security operation". Calls and warnings sent through communication channels are used.


ODESA SEA PORT
Inject 1.3.2



Response to Inject 1.3.3

Most notably, participants agreed a decision by political leadership would be required to address the attempt by the Bastan Navy to stop the tanker. Furthermore, political leadership would decide if the Senta State Border Guard Sea Service (or alternate service) should be tasked to escort commercial ships arriving/departing from Senta ports.

While not directly addressed by the participants, Bastan Navy activities were labelled by the following terms throughout the vignette: 'provocative', 'violations', 'violations of freedom of navigation', 'obstruction of navigation' and 'aggressive'. The participants did not articulately address what departments/agencies are responsible for addressing each term in accordance with Senta national law and differentiating the definition (for example) of a 'provocation' versus an 'aggressive action'.

5.2. Vignette 2: Low-intensity Hybrid Operations

Weather conditions in the Southern regions of Senta deteriorated at the beginning of February. The wind speed reaches 50 m/s index causing considerable damage, namely in the Odesa region.

Bastan's import restrictions on Senta's agriculture, manufacture and metal products, as well as fuel, chemicals and petroleum products contribute to the decline of Senta's economy which has already been in recession. Pro-Bastan activists use the economic downturn as a chance to intensify protests against Senta's government. Social tensions reached their peak when news about Odesa City Council's decision concerning secession of the Odesa region from Senta has spread via the Internet.

The work of Odesa Sea Port is continuously disrupted by the actions of pro-Bastan activists and incidents in the cyber-security domain. Moreover, Senta's civilian and coast guard vessels reported technical issues in their navigating system.

Furthermore, Bastan's vessels act aggressively against Senta's fishing boats. Coast guard ships of Bastan intimidate and threaten cargo vessels of Senta and foreign states as well. Recently, Bastan Naval Forces provided support to the illegal gas exploration and drilling rigs installation operation within the territory of Senta's EEZ. The 24-hour security guard patrol of Bastan's Navy was established around the rigs.

Response to Vignette 2

Participants collectively agreed Senta must ensure safety of navigation within territorial waters and including the economic exclusion zone (EEZ). Participants had diverging perspectives regarding how Senta would achieve the objective. A reoccurring theme during discussions was identifying what Senta department/agency/Armed Force would lead a coordinated response and under what law/authority. It was agreed that the Senta Maritime Border Guard Service would identify oil spills and other similar incidents, and that the rescue and response operations would be handled by the State Emergency Service in conjunction with the Ministry of Infrastructure in cooperation with other relevant agencies.

The syndicate regarded Bastan Navy and Coast Guard actions as intentional to create a negative image of Senta as a maritime state and to adversely impact the economy.

Participants agreed the Ministry of Foreign Affairs (MFA) would lead the effort to appeal to the international community for assistance. The MFA would be tasked to: diplomatically prevent further escalation of the conflict(s), leverage international law and support from the international community to force Bastan to recognize and cease activities in Senta's EEZ and attempt to slow Bastan's operations in order to increase decision making time for Senta political leadership. In the meantime, participants generally encouraged increasing the quantity of defensive forces on Totara Island as a preventative measure.

Inject 2.3.1: Day 26: January 31, 10:00

Several Senta's civilian and coast guard ships in the Noir Sea near Odesa Sea Port report anomalies with their GPS-derived position. Similar disruptions are reported by Zestan civilian ships. Senta's air traffic operators report that signals from some passenger planes flying over Senta's coast in the Noir Sea are lost. A vessel under the flag of Comoros has been discovered in the EEZ of Senta, carrying out electronic warfare and intelligence activities in the interest of Bastan.

Response to Inject 2.3.1

Participants collectively agreed Senta must ensure safety of navigation within territorial waters and including the economic exclusion zone (EEZ). Participants had diverging perspectives regarding how Senta would achieve the objective.

The Maritime Security Syndicate discusses challenges in the "Noir Sea" during the NATO CORE 20 TTX in Odesa, Ukraine.

Inject 2.3.2: Day 43: February 17, 10:00

Tanker belonging to Senta suddenly loses control and collides into Bastan's cargo ship in EEZ of Senta, causing the discharge of oil and a major fire. Some casualties are reported. Bastan authorities accuse Senta authorities of sabotage.

Response to Inject 2.3.2

A reoccurring theme during discussions was identifying what Senta department/agency/Armed Force would lead a coordinated response and under what law/authority. There was mutual understanding the Senta Border Patrol Sea Service would direct rescue operations and respond to the oil spill. Notably, the participants referenced leveraging the Air Force for the first-time in the exercise to support search and rescue operations (pending approval by political leadership).

Inject 2.3.3: Day 46: February 20, 17:00

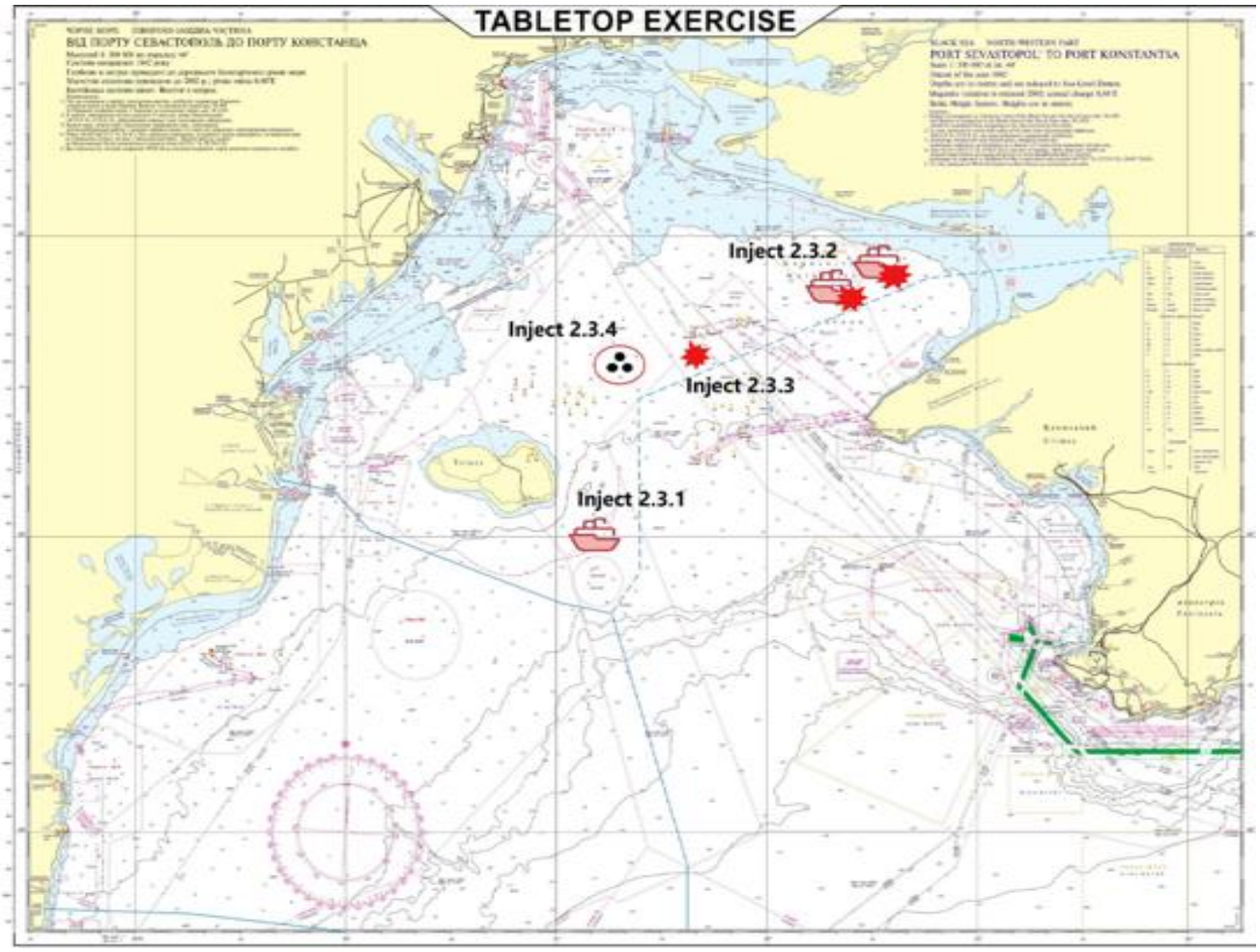
Senta's coastal guard ships inform about Bastan's Navy actions in the Noir Sea. In recent time, Bastan has started installing gas jack-up drilling rigs within the territory of Senta's continental shelf. Bastan's navy ships are patrolling around these gas rigs.

Response to Inject 2.3.3

The syndicate regarded Bastan Navy and Coast Guard actions as intentional to create a negative image of Senta as a maritime state and to adversely impact the economy.

Inject 2.3.4: Day 48: February 22, 07:00

The Bastan Navy and coast guard intimidate Senta and Zestan civilian cargo ships heading to Senta's ports in the Noir Sea while being in EEZ of Senta and demand their course change back to the outer border of Senta's EEZ. According to Bastan media sources, Senta's civilian cargo ship attempts to ramp into Bastan's navy ship deliberately. According to Bastan's media reports, under such circumstances, Bastan's authorities have decided to increase its Naval presence to protect its ships and interests from provocative actions of Senta.



Response to Inject 2.3.4

Participants agreed the Ministry of Foreign Affairs (MFA) would lead the effort to appeal to the international community for assistance. The MFA would be tasked to: prevent further escalation of the conflict(s), leverage international law and support from the international community to force Bastan to recognize and cease activities in Senta's EEZ and attempt to slow Bastan's operations in order to increase decision making time for Senta political leadership. In the meantime, participants generally encouraged increasing the quantity of defensive forces on Totara Island as a preventative measure.

5.3. Vignette 3: Conflict Phase: High-intensity Hybrid Operations

Senta's critical infrastructure experiences a wide range of kinetic and non-kinetic attacks. Disruptions occur on the natural gas transmission pipeline in the Southern gas transit corridor, affecting supply to the Southern region of Senta and the neighbouring foreign states. Moreover, there is a threat of disruption of the heating season not only in the southern part of Senta but in Kharkiv and Luhansk regions as well, in particular those heavily depending on the gas supplies from Bastan.

In the South of Senta, there is a one-third increase of the number of emergencies, fires and accidents caused by arson and terrorist attacks using explosives, which in turn has led to a significant increase in the number of casualties. A significant incident is suspected in PJSC 'Odesa Portside Plant' where the considerable release of hazardous chemicals is reported.

Information on disruptions in the South Senta NPP operation is disseminated. Bastan's media blames Senta's authorities for the release of radiation. Almost at the same time, information about the attack against hydroelectric pumped storage power plant attack is being spread.

Massive cyber-attacks disrupt the operation of the Odesa Sea Port, including transportation and cargo handling. The branches of Oshchadbank and PrivatBank banking systems in the Odesa region were attacked.

In a month after the first cyber-attack on Liebherr's internal network in Germany, there have been a series of minor cyber-attacks on the Liebherr's port cranes all over Europe.

In the maritime domain, Bastan's Navy ships are increasing their presence in the Senta's EEZ, using navy exercises and interrupting the international passenger and cargo sea transhipment.

Response to Vignette 3

Syndicate members unanimously agreed Bastan's actions illustrate an obvious objective to cause economic damage to Senta. While participants did not all attribute the mine-related explosions to Bastan's actions, Senta Security Services would be charged to investigate the mines/mining as a terrorist attack and conduct anti-terrorist operations in the vicinity of the Sea Port Yuzhnyi. In parallel, the Ministry of International Affairs would request for NATO to send a mine countermeasures task group to the area. However, the participants did not clarify the command-and-control structure for NATO forces within the Senta EEZ, and the collaboration/coordination required amongst NATO forces and the Security Services conducting anti-terrorist operations in the same vicinity was not clarified.

In an effort to be less-reactive, the syndicate recognized Bastan's actions may have a collective objective to create an operational environment for Bastan to conduct a much larger operation. As a result, the syndicate proposed the National Security Council would task the sea services (including the Navy) to: ensure the safety of shipping, increase military presence in the coastal territories and Totara Island. At the same time, as throughout the exercise, syndicate members believed a three-pronged approach including a defensive military posture, focus on de-escalation and international diplomacy would prove effective. Every time the situation changed, the participants discussed and determined the roles and authorities of every Senta department/agency.

At this point in the exercise, participants agreed the Senta President's office would gather the NSC to request the implementation of martial law in the affected region. Participants had different beliefs concerning how martial law would impact/influence Bastan's actions and/or objectives. Martial law was perceived by many as another example of a defensive-like military posture. Therefore, participants had different views on how martial law could be leveraged to plan/coordinate offensive operations or what conditions needed to be met and by whom (e.g. Bastan's forces, Senta Navy, etc.) in order to rescind martial law.

Inject 3.3.1: Day 53: February 27, 11:00

Two explosions sink two cargo vessels owned by Senta and Zestan, proceeding to Sea Port Pivdennyi. Two buoyant WWII contact mines are detected by surveillance planes and eliminated by the Senta's Navy. The government of Zestan releases initial technical evidence compromising the assumption about old contact mines: all damage is located deeper under the hull, near the stern, and all explosions hit the engine room. Some international shipping companies declare Senta's EEZ as dangerous for shipping.

Response to Inject 3.3.1

Syndicate members unanimously agreed Bastan's actions illustrate an obvious objective to cause economic damage to Senta. While participants did not all attribute the mine-related explosions to Bastan's actions, Senta Security Services would be charged to investigate the mines/mining as a terrorist attack and conduct anti-terrorist operations in the vicinity of the Sea Port Yuzhnyi. In parallel, the Ministry of International Affairs would request for NATO to send a minesweeping task group to the area. However, the participants did not clarify the command-and-control structure for NATO forces within the Senta EEZ, and the collaboration/coordination required amongst NATO forces and the Security Services conducting anti-terrorist operations in the same vicinity was not clarified.

Inject 3.3.2: Day 54: February 28, 09:00

Bastan's Navy declares a shooting and exercise area dangerous and blocks a sea route to Odesa Sea Port. An intense LIVEX, including the use of various arms systems, has been ongoing for two weeks and is situated in the vicinity involving merchant vessels navigating through the area - disrupting shipping activities.

Response to Inject 3.3.2

In an effort to be less-reactive, the syndicate recognized Bastan's actions may have a collective objective to create an operational environment for Bastan to conduct a much larger operation. As a result, the syndicate proposed the National Security Council would task the sea services (including the Navy) to: ensure the safety of shipping, increase military presence in the coastal territories and Totara Island. At the same time, as throughout the exercise, syndicate members believed a three-pronged approach including a defensive military posture, focus on de-escalation and international diplomacy would prove effective. What Senta departments/agencies/Armed Forces would lead the approach and how the efforts between/amongst stakeholders would be coordinated in–parallel (or consecutively) was not road mapped.

Inject 3.3.3: Day 55: March 1, 12:00

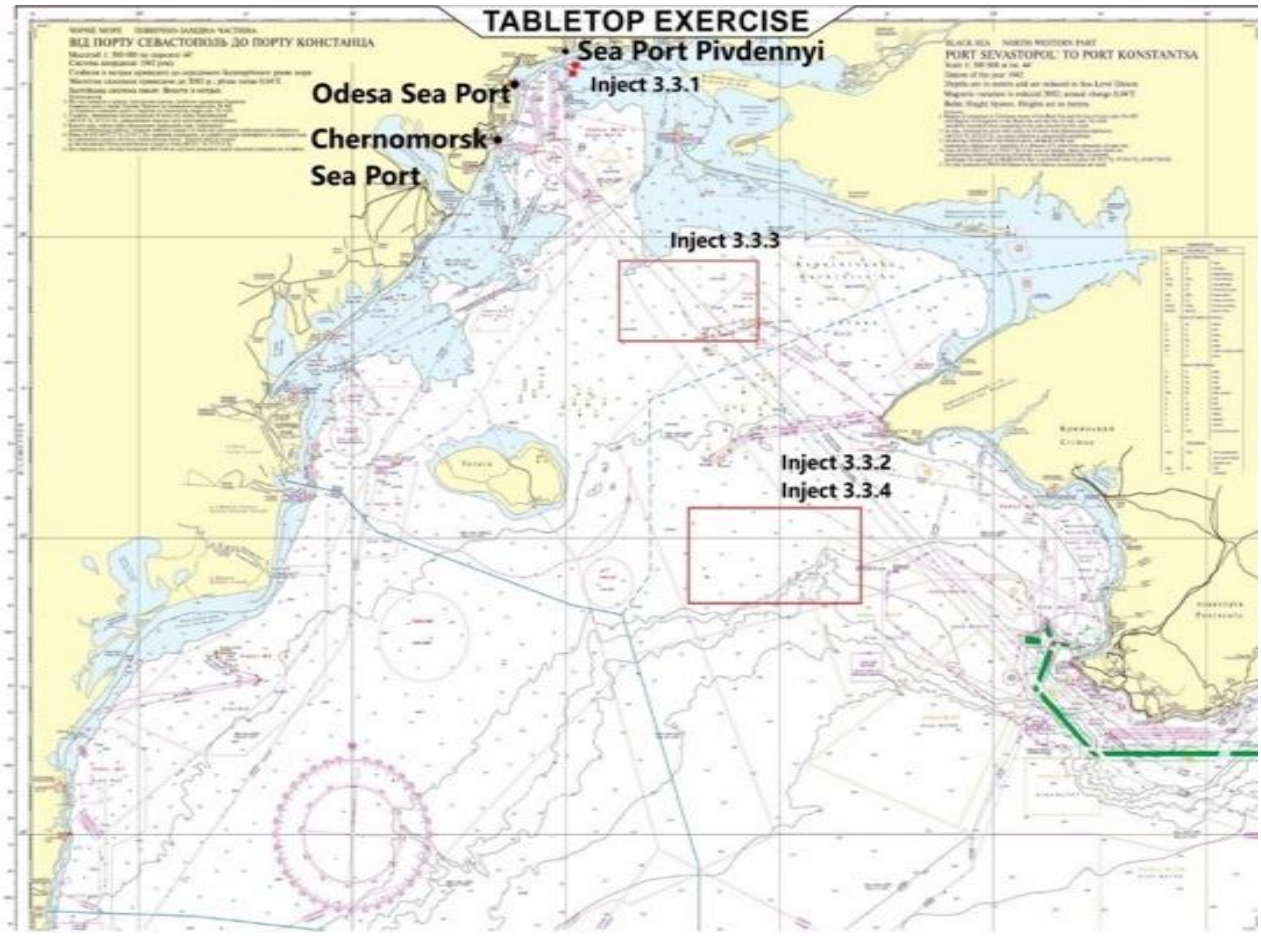
Bastan establishes a control zone in Senta's EEZ where ships bound to Senta are stopped and searched by the Bastan Navy, the coast guard, or both. Motivation for these acts, as announced by Bastan, is a suspected terrorist threat against undefined strategic targets. Ships are subjected to random controls. Delays are ranging from five hours to two days. The average waiting time per vessel is 20 hours.

Response to Inject 3.3.3

Syndicate did not provide explicit response to this inject.

Inject 3.3.4: Day 55: March 1, 16:00

Bastan's Navy extends exercise activities and declares significant parts of Senta's EEZ area as dangerous. Significant LIVEXs disrupts access to most of Senta's ports in the Noir Sea. As a result, major ferry and liner shipping lines halt their services, and some companies suspend activities. The ferry ship connection with Zestan is disrupted.



Response to Inject 3.3.4

At this point in the exercise, participants agreed the Senta President's office would gather the NSC to request the implementation of martial law in the affected region. Participants had different beliefs concerning how martial law would impact/influence Bastan's actions and/or objectives. Martial law was perceived by many as another example of a defensive-like military posture. Therefore, participants did not socialize how martial law could be leveraged to plan/coordinate offensive operations or what conditions needed to be met and by whom (e.g., Bastan's forces, Senta Navy, etc.) in order to rescind martial law.

5.4. Vignette 4: Hybrid Warfare

Tensions between Bastan and Senta have reached the highest level ever. Senta's military intelligence reported an unprecedented number of military build-up in Bastan Navy's bases in the Noir Sea. A significant number of provocative accidents have started to occur on Totara Island. Reports of the loss of GPS and GSM signals on the island. The Internet connection on the island was disrupted.

At the same time, Senta continues to experience a growing number of cyber-attacks against governmental and local institutions, and critical service providers. Bastan's and Senta's media aggressively reports about the inability of Senta's central and local authorities to provide critical services for the population. Moreover, top commanders of Senta's armed forces in Kyiv and Navy officials in Odesa and Totara Island received e-mails from unconfirmed accounts with a direct warning 'not to follow orders of Senta's political authorities, or they and their families will be in danger'.

Social media is full of reports and active discussions about the possible separation of the South part of Senta. The same news is being spread via official web pages of regional councils. The above leads to pressure and tensions inside governmental institutions, law enforcement agencies, and armed forces. In the last 24 hours, street manifestations against the Senta government intensified dramatically, namely in the central cities of southern regions: Odesa, Mykolaiv and Kherson. As a result, the government is overstretched, and the population is confused.

Against the background of significant cyber disruptions, psychological pressure, the spread of misinformation, and growing street manifestations in southern regions, suddenly a considerable number of military forces without insignia launched on the Totara Island. The access to the Port of Totara Island is blocked by the cargo ships with no State flag identification. The access by water to the Totara Island is cut off.

Drilling rigs for hydrocarbon production of Totara Island located in the Senta's EEZ were occupied and now are under the full control of armed men with no State identification.

Response to Vignette 4

Syndicate members agreed that since the armed men did not have insignias, Senta would identify them as terrorists. As a result, an anti-terrorism operation(s) would be conducted under martial law to remove the armed men. In this situation the syndicate clarified that the anti-terrorist operation should be coordinated by the Security Service.

After three consecutive injects which included offensive operations conducted by armed men with no insignia, participants were (debatably) internally (within Senta) focused on protecting critical infrastructure and relocating additional forces on Totara Island. As a result, the Ministry of Foreign Affairs and other non-military department/agencies were referenced less in discussions as collaborators and tools for the whole of Government approach to achieve a mutual objective (e.g. arrest the armed men, regain access to the South-Western naval headquarters, etc.) Similarly, participants debated the value and likelihood of receiving international support (including from NATO). As a result, some participants increasingly suggested addressing and engaging the threat posed by the armed men via anti-terrorism/military operations as opposed to strengthening interdepartmental and civil-military cooperation to counter the hybrid threats.

Inject 4.3.1: Day 56: March 2, 05:00

Armed men occupy eight gas rigs off Totara Island in the EEZ of Senta without insignia who used helicopters to land on the rigs and took them over. Bastan's Navy establishes a control zone around rigs, namely in Shtormov and Halitsyno gas deposit areas. Civilian ships and aeroplanes report significant disruptions of GPS signals in the Noir Sea region.

Response to Inject 4.3.1

Syndicate members agreed that since the armed men did not have insignias, Senta would identify them as terrorists. As a result, an anti-terrorism operation(s) would be conducted under martial law to remove the armed men. The lead military service and/or coordination required to conduct the operation was not further defined.

Inject 4.3.2: Day 58: March 4, 02:00

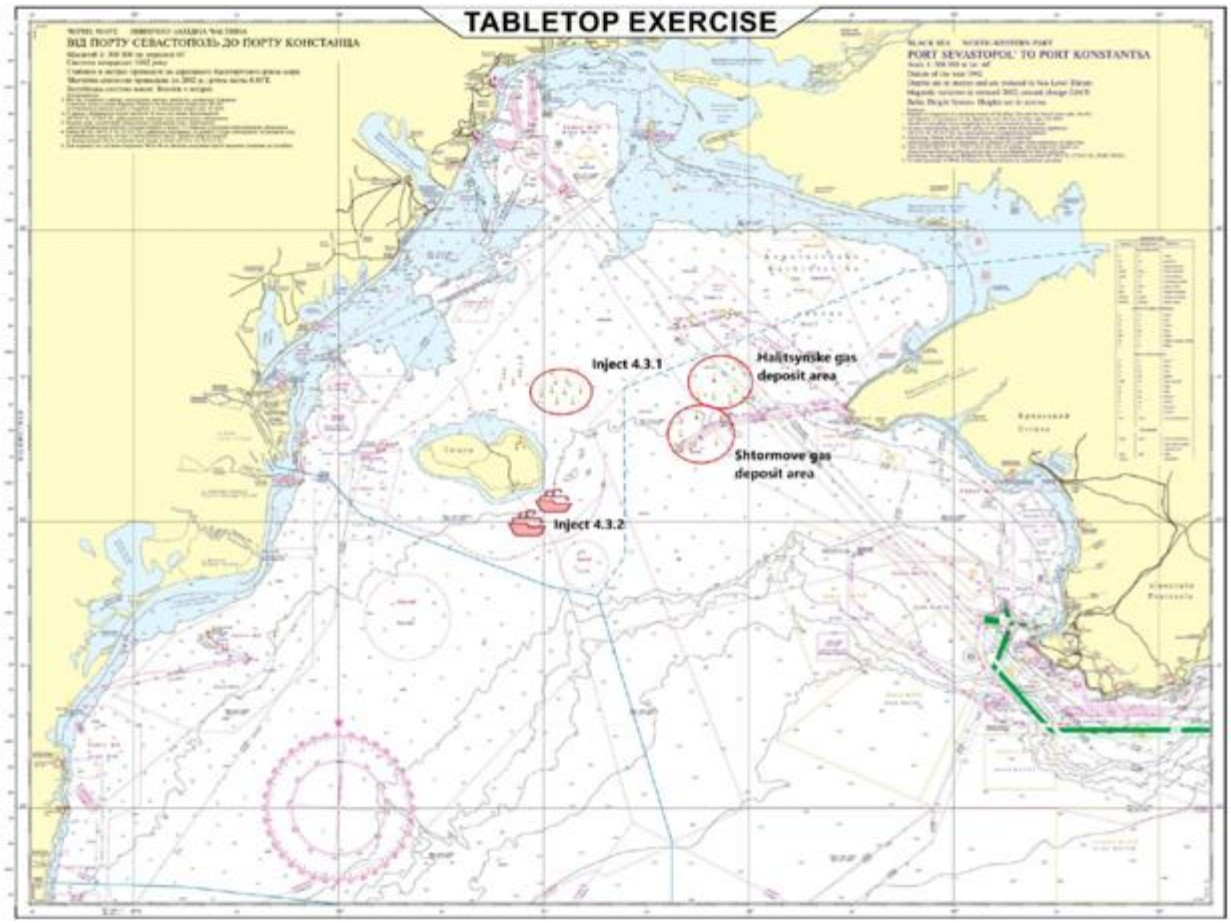
Since the establishment of the control zone in Senta's EEZ, the control of SLOCs by Bastan continues. A significant number of heavily armed men without insignia and pro-Bastan activists land on Totara Island at night by helicopters and civilian cargo ships. Reports about the takeover of local institutions and major Senta's naval base on the island. Cargo ships with no State flag identification are used to block access to the naval base completely.

Response to Inject 4.3.2

Syndicate members sought diplomatic means to end the crises, but in the meantime, the economic situation in Senta continued to deteriorate due to the disruption of port operations, maritime traffic, sabotage, etc. Primarily due to the dependence of syndicate members on diplomacy and support from NATO members and partner nations, the scope of a perspective military operation continued to increase (to remove the Bastan and unidentified forces from Senta territory [including the EEZ]), the crisis continued to escalate, and the resilience of Senta's critical infrastructure and preparedness again (additional) hybrid threats continued to be diminished.

Inject 4.3.3: Day 58: March 4, 13:00

Military vessels of Senta's Navy Forces located in the Totara port area are blocked and seized by armed men with no insignia. Some casualties are reported. Senta's central government and military authorities completely lose access to its South Western naval headquarters situated on Totara Island. The connection with the EEZ of neighbouring states is disrupted.



Response to Inject 4.3.3

After three consecutive injects which included offensive operations conducted by armed men with no insignia, the participants were (debatably) internally (within Senta) focused on protecting critical infrastructure and relocating additional forces on Totara Island. As a result, the Ministry of Foreign Affairs and other non-military department/agencies were referenced less in discussions as collaborators and tools for the whole of Government approach to achieve a mutual objective (e.g., arrest the armed men, regain access to the South-Western naval headquarters, etc.) Similarly, participants debated the value and likelihood of receiving international support (including from NATO). As a result, participants increasingly suggested addressing and engaging the threat posed by the armed men via anti-terrorism/military operations as opposed to strengthening interdepartmental and civil-military cooperation to counter the hybrid threats.

5.5. Vignette 5: Post-Crisis Stabilisation

The present vignette focuses on the post-crisis and recovery stabilisation process. The post-crisis stabilisation takes place after the end of the crisis scenario – from March 7, 20YY. Crisis management issues are to be discussed, as well.

Each syndicate will be presented with several questions for the post-crisis stabilisation discussion.

1. Is maritime security legislation comprehensive (sufficient) to date? If not, what are the priority areas for improving it in the post-crisis analysis?

Response

Participants discussed the need to develop and adopt country's Maritime Security Strategy, complete the legislative work on demarcation of country's sea borders with participation of international mechanisms, as well as amend the current legislation and develop new legislation to ensure protection of the national interests at sea. Participants also proposed to develop and implement a cooperative maritime security strategy with NATO and partner countries in the Azov - Black Sea region.

2. What are the issues of ensuring the proper (continuous) interaction of the security and defence sector components and the civilian component (State Border Service, Naval Forces, State Emergency Service, Seaport Administration and Port Managers, State Transport Security Service, Marine Search and Rescue Service, State Fisheries Agency, State Environmental Inspectorate) for ensuring post-crisis maritime security?

Response

At the beginning of the exercise, multiple syndicate members were adamant proper interaction of the security and defense sector components and the civilian component is seamless in a pre and post-crisis maritime security environment. However, as the exercise progressed, a few participants expressed contrary views about interactions amongst stakeholders specifically regarding roles and responsibilities within the security and defense sector. Since syndicate membership consisted of predominantly military members, participants frequently also focused on interaction of the security and defense sector components. Most notably, syndicate members were not able to collectively agree on the roles and responsibilities to interact independent of legislation/laws. Moving forward, syndicate members acknowledged the benefit of further exploring interaction between/amongst civilian components as well (for ensuring post-crisis maritime security).

3. What are the problems with public-private sector interaction in maritime security? What are the options for settlement?

Response

Once again, due to limited representation of syndicate members with private sector experience, problems were frequently raised concerning public-private sector interaction. Since syndicate members frequently referenced the importance of the maritime sector to the Senta economy, multiple syndicate members acknowledged increased public-private sector interaction in maritime security is required. Furthermore, Senta departments/agencies would benefit from training regarding the private sectors perception of maritime security and its importance to the industry.

5.6. Key Takeaways

Requirement for Martial Law in the Hybrid Threat Environment. The declaration of martial law was debated by the Syndicate based upon independent hybrid actions and the culmination of multiple hybrid actions. **Recommendation:** Identify indicators of hybrid threats which will independently or collectively result in the declaration of martial law. Adopt legislation as hybrid threats evolve. Ongoing monitoring and identification of new indicators of non-military threats affecting maritime interests of the nation. Determine the course of action of the defense and security sector based on these threats. Develop new ways to apply aspects of martial law in a hybrid threat environment without having to declare martial law, such as increasing the anti-terrorism threat level and using anti-terrorist operations as a counter.

Continuous Hybrid Threat Environment. Syndicate members sought diplomatic means to end the crises, but in the meantime, the economic situation continued to deteriorate due to the disruption of port operations, maritime traffic, sabotage, etc. **Recommendation**: Taking into account the new Concept of Ensuring the National Resilience System, agency-specific documents should clarify the procedure and ensure the implementation of crisis response measures. In particular, include political, informational, economic, socio-humanitarian, military and other measures to minimize the threats, impact and consequences of hybrid actions.

Defining Hybrid Threats as a Means to Mitigate Hybrid Actions. Throughout the exercise, syndicate members often struggled with identifying applicable maritime laws and the appropriate enforcement ministry, based upon ambiguous definitions of various hybrid threats. **Recommendation**:The identified hybrid threat indicators should be aligned with those used in NATO member countries, taken into account in relevant crisis response plans, policies and procedures, in order to eliminate ambiguity between national ministries and NATO members.

Defense Capabilities and Capacity of NATO Members, Partner Nations, and International Organizations. When political and/or military leadership determined additional defense capabilities and capacity were required to supplement the Armed Forces and/or fill capability gaps, the syndicate members leveraged NATO Members, Partner Nations, and/or International Organizations. **Recommendation**: In preparation for coordinating operations between/amongst Ukraine Armed Forces and NATO members, partner nations, and international organizations, Ukraine should identify capability gaps taking into account new changes in threats to critical infrastructure and supply chains and include the stakeholders in the national crises management. At the same time provide for simplification of mechanisms for attracting foreign units, funds and resources.

Comprehension of Domestic and International Maritime Laws to Counter Hybrid Threats. Throughout the exercise, the adversary exploited international and domestic laws to validate and/or increase the hybrid threat of its forces operating within Ukraine's Economic Exclusion Zone. In Ukraine, its civilian-led Government has operational control of the military to conduct conventional warfare. In the adversary's civilian-led Government, it has operational control of the military to conduct hybrid actions and conventional warfare. As a result, each country's Armed Forces operate differently in how they employ plans, policies, and procedures. **Recommendation:** Planning and implementing of maritime security measures should be carried out taking into account the forecast of the enemy's actions based on its current legislation and the possible abuse or disregard for international law.

Requirement for Time-Late Common Operational Picture. In order to enhance resilience of critical infrastructure and preparedness against hybrid threats, all stakeholders are likely to contribute to a common operational picture for maritime security. **Recommendation**: To increase the level of awareness of the maritime situation, reduce the time for decision-making on responding to hybrid threats at sea, improve inter-agency procedures for collecting, processing and summarizing information and provide for the establishment of a national coordination center for maritime security. Ensure involvement of foreign personnel in the work of the center to increase the level of interoperability with NATO member countries

Multi-Domain Approach to Increase Intelligence, Surveillance and Reconnaissance (ISR) Against Hybrid Threats. The syndicate discussed the need for a multi-domain integrated ISR system to counter hybrid threats. **Recommendation**: To ensure involvement of all components of the security and defense forces, civilian organizations and institutions that carry out tasks in the maritime sphere (at sea), in the interests of covering the surface and underwater environment and the exchange of information in this area. To do this, create a state integrated ISR system in the waters of seas and river basins.

Armed Forces Posture in an Unconventional Environment. Recommendation: During planning of crisis response ensure necessary capabilities to protect national interests, including economic, political and others, their sustainment and employment according to the identified preparedness levels.

6. Syndicate 4: STRATCOM

6.1. Vignette 1: Pre-conflict Phase: Hybrid Influencing

Political and economic intimidation against Senta by Bastan authorities is growing. On the basis of the gas transit agreement, which has been signed by Bastan and Senta last year, the Bastan government accused Senta of infringing agreement provisions. Senta denies any violations. However, Bastan's media and some Senta's media controlled by Bastan keep spreading the messages about Senta's violation, stressing the importance of the corresponding agreement for Europe's energy security as the gas transit to European countries is partially ensured through the territory of Senta.

The situation is aggravated by the fact that there is no new contract for gas supply between Bastan and Vela. Given disputes over contractual provisions, Bastan temporarily substantially reduces gas supplies to Vela. Vela maximally draws gas from the transit pipeline, limiting gas supplies to Senta's customers in the Odesa region, near the border with Romania.

Meanwhile, Bastan inflicted import restrictions on Senta's agriculture, manufacture, and metal products, as well as fuel, chemicals, and petroleum products. Besides, Bastan ceases to supply oil products to Senta with automotive, railway transport, and pipelines.

Three websites were found on the Internet with identical visual designs and features of the official websites of Senta GTS Operator, PSG Operator, and Naftogaz Company. Moreover, e-mails with phishing features and attached Microsoft Word text documents have been found in the e-mail boxes of Senta's regional government agencies.

Media reports were released about the powerful cyber-attack on Liebherr's internal network in Germany. As a result, port cranes at the Poti Sea Port in Zestan have stopped working.

From the middle of December, Senta's coast guards are regularly reporting about the Bastan's Navy presence in the Senta's EEZ. It is reported that Bastan conducted military exercises in the Noir Sea in the nearest vicinity of the fairway passage of merchant and passenger ships from/to ports in the Odesa region.

The Strategic Communications Syndicate discuss exercise inject responses during NATO COHERENT RESILIENCE 20 TTX in Odesa, Ukraine.

Inject 1.4.1: Day 1: January 6, 11:00

A year after signing the gas transit agreement, Bastan authorities accuse Senta of violating the agreement – warning to terminate the contract and halt gas supplies through Senta territory. Bastan's media intensifies the broadcast of messages about Senta's breach of gas transit agreement underlying a narrative that Senta might keep hostage not only its population but also European countries. This information is also broadcasted by some TV news channels in EU countries.

Response to Inject 1.4.1

There was debate by the participants as to what message to push out and how to do it. At this phase, is there a crisis, and should they treat it like a crisis? Fighting the false narrative coming out of Bastani media was their priority, via diplomatic and mass media channels. However, there was broad acknowledgement that there was no clear policy as to which agency should be the lead on this goal of narrative pushback, which leads to uncertainty about what the message should actually be. Because Senta lacks a defined process to create a crisis response team, there was also much discussion on who makes the decision that there is a crisis and then creates an ad hoc crisis response team. Many participants got stuck on policymaking in the moment and were not thinking strategically. Leaders reminded participants that this is only part of Bastani hybrid actions, and that the narrative intended to make Senta look unreliable as a transit country was only the beginning. Participants knew what to do, but there was a lack of agreement as to how to do it. This facilitated the realization that Senta needs a STRATCOM agency at the ministerial level, so that its messaging on countering Bastan narratives, was clear, non-contradictory, and addressing the overall picture.

Inject 1.4.2: Day 14: January 19, 02:00

Bastan social media actively discusses that suspected cyber-attacks that have disrupted major banks of Senta (PrivatBank, Oschadbank) and previously central governmental institutions were intended to cover the money laundering of the corrupted government and business.

Response to Inject 1.4.2

Here relevant agency representatives stepped forward to address this false information. Discussion centered around the banks issuing a statement on the disclosure of information about cyberattacks as well as on the need to create an information advantage and the ability to inform society in an efficient manner. Refutation of these false narratives seemed to be the focus, with talk of involvement of public organizations to refute fakes (a series of publications), holding round tables. Additionally, the syndicate identified the National Security and Defense Council as the lead agency who should determine the level of threat and send information to the relevant cabinets. They decided that the police should issue a statement on the investigation of information about cyber-attacks. Again, the issue wasn't the messaging, but how to get the message to the different audiences that needed to hear pushback against these manufactured Bastani narratives.

Inject 1.4.3: Day 16: January 21, 11:00

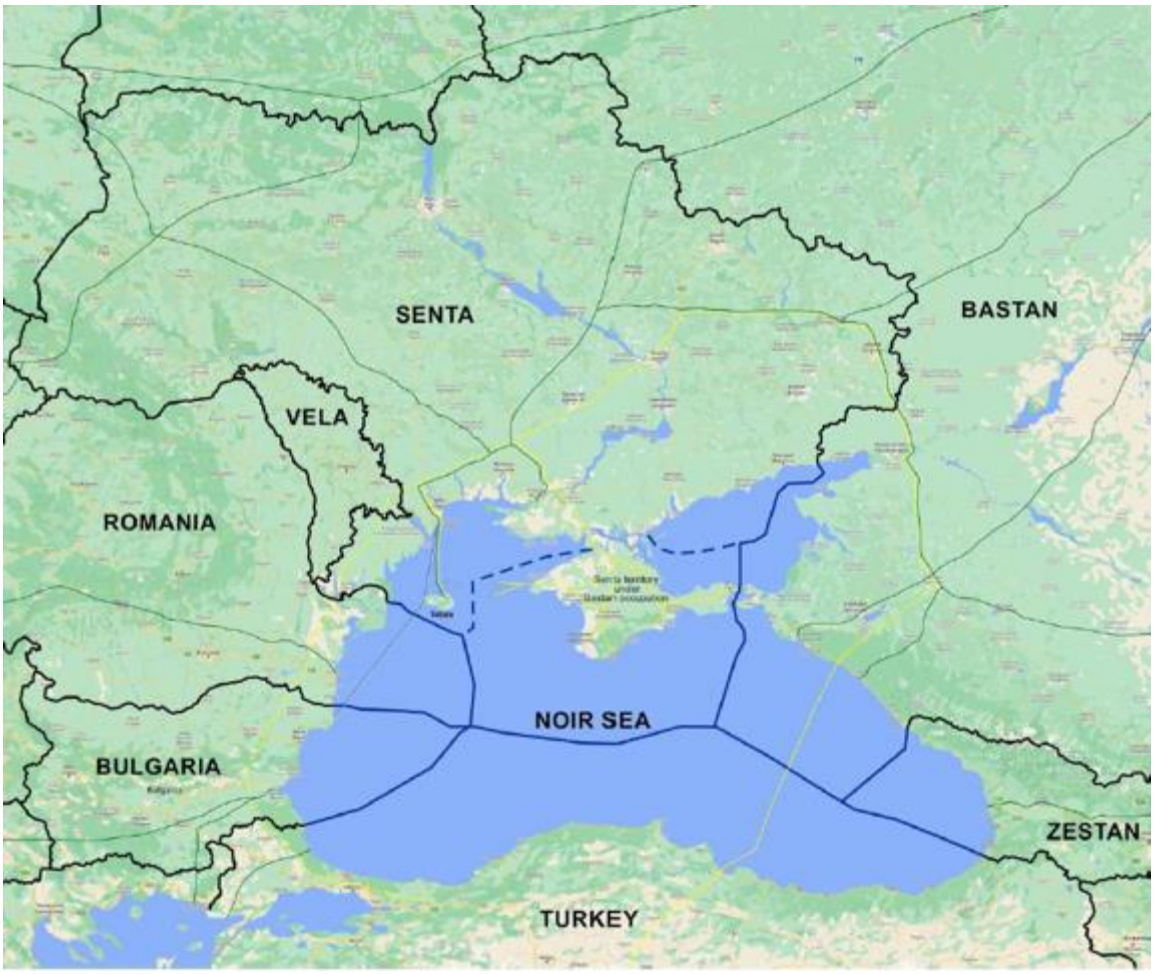
Many customers add many social media posts about the incorrect work of the utility billing and payment centres, many indignant consumers with erroneously accrued debt.

Response to Inject 1.4.3

Participants stressed the need for the government to come out forcefully to help mitigate panic about the false stories about utility billing. The NDSC and MOI were named several times as the agencies to be the ones to address these narratives and pushback. Also, the suggestion of the creation of a special agency came up, with others imploring that there needs to be a ministerial-level STRATCOM center that coordinates communications between relevant agencies at the national, state, and local level. There was also talk of judging the severity of this threat, and then having influencers from the private sector help with the pushback of the narrative on the billing anomalies. There is not a need for help here from the international community, and the narrative should originate internally from Senta authorities, as there was worry that reliance on foreign experts or assistance would help the Bastani narrative. Again, the issue here was the how to message and how to target relevant audiences, not the messaging itself. The syndicate struggled with continuing lack of clear understanding of who is responsible to direct and coordinate crisis response activities, and thus who should coordinate the information response across the various ministries and agencies involved.

Inject 1.4.4: Day 21: January 26, 06:00

A significant number of leaflets and flyers are distributed to people's mailboxes in Odesa and other regional cities – asking people to rise against corrupt local governments.



Response to Inject 1.4.4

The SBU monitors and identifies threats, and it was acknowledged that this was needed in order for them to create a good counternarrative. It was then suggested that the SBU and Regional State Administration monitor the situation in the region, with the RSA monitoring rallies and the main false messages being spread, and the SBU identifying the threat and updating the internal audiences on the situation frequently. Use of telephone hotlines, social media, and mobile phone companies is suggested to make sure that the domestic messaging is able to reach as many people as possible. Ultimately, the need for a nationally coordinated STRATCOM center became evident again, and the need to not only be concerned with the domestic audience, but the need to influence foreign allies and partners, as well as adversarial audiences.

6.2. Vignette 2: Low-intensity Hybrid Operations

Weather conditions in the Southern regions of Senta deteriorated at the beginning of February. Wind speed reaches 50 m/s index causing considerable damage, namely in the Odesa region.

Bastan's import restrictions on Senta's agriculture, manufacture and metal products, as well as fuel, chemicals and petroleum products contribute to the decline of Senta's economy which has already been in recession. Pro-Bastan activists use the economic downturn as a chance to intensify protests against

Senta's government. Social tensions reached their peak when news about Odesa City Council's decision concerning secession of the Odesa region from Senta has spread via the Internet.

The work of Odesa Sea Port is continuously disrupted by the actions of pro-Bastan activists and incidents in the cyber-security domain. Moreover, Senta's civilian and coast guard vessels reported technical issues in their navigating system.

Furthermore, Bastan's vessels act aggressively against Senta's fishing boats. Coast guard ships of Bastan intimidate and threaten cargo vessels of Senta and foreign states as well. Recently, Bastan Naval Forces provided support to the illegal gas exploration and drilling rigs installation operation within the territory of Senta's EEZ. The 24-hour security guard patrol of Bastan's Navy was established around the rigs.

Inject 2.4.1: Day 22: January 27, 08:00

Under the pretext of deteriorating economic situation and rising prices for petroleum products and fuel, pro-Bastan activists start blocking main roads, port facilities, and fuel terminals in Odesa. Bastan's media accuses Senta's law enforcement agencies of using force and killing dozens of protesters.

Response to Inject 2.4.1

The false Bastani narratives are escalating, with Bastani media announcing that Senta police are killing the protesters in the Odesa region. The syndicate agrees that this is a national issue and not just a regional one, and that reactions and messaging must be coordinated across the national and regional levels. Talk of the creation of a national STRATCOM center continues, with more tangible ideas as to the structure of this agency. The mobilization of journalists, opinion leaders, and the Ministry of Foreign Affairs were suggested as the top actors in this inject, although the process of mobilizing and coordinating these actors was not discussed as clearly. Having the SBU block Bastani social media and then spreading truthful information was also suggested, but the process and legality of these suggestions faced pushback.

Inject 2.4.2: Day 24: January 29, 12:00

The website of Odesa City Council states that regional authorities decided to declare independence from Senta and become the Odesa Autonomous Republic. Appeal to Bastan's authorities for help.

Response to Inject 2.4.2

Participants felt that this false narrative would be easy to debunk, and a suggestion of the SBU being the main actor pushing back against this narrative was suggested. It was less clear as to how this would be achieved effectively. SMEs also suggested how to tackle these escalating disinformation campaigns by Bastan, reminding them to think strategically. SMEs also encouraged them to think about messaging to three audiences: reassure the domestic audience, show resolve to the international community, and deter Bastan's narratives. Up to this point, the syndicate had been thinking about the first two, but not about the third. The syndicate had good ideas as to what to do but needed more structure and more direction in order to be more effective at STRATCOM.

Inject 2.4.3: Day 40: February 14, 20:00

Media and social media have information on the public availability of information on utility billing, indicating customers' personal data (such as name, address, telephone number, e-mail).

Response to Inject 2.4.3

With suggestions from SMEs on the previous inject fresh in memory, syndicate members focused on the need to quickly determine the validity of this story, as people may panic if their personal information has been compromised by hackers. Truthful information must be released immediately and updated frequently so as to stay ahead of Bastan's disinformation campaign. Here the internal audience is the top priority. Crisis is already happening in other domains, and STRATCOM must think about the possible next moves by Bastan's information operators. The syndicate also identified that the lack of power, heating, and food was likely a more pressing concern for their internal audience.

Inject 2.4.4: Day 43: February 17, 10:00

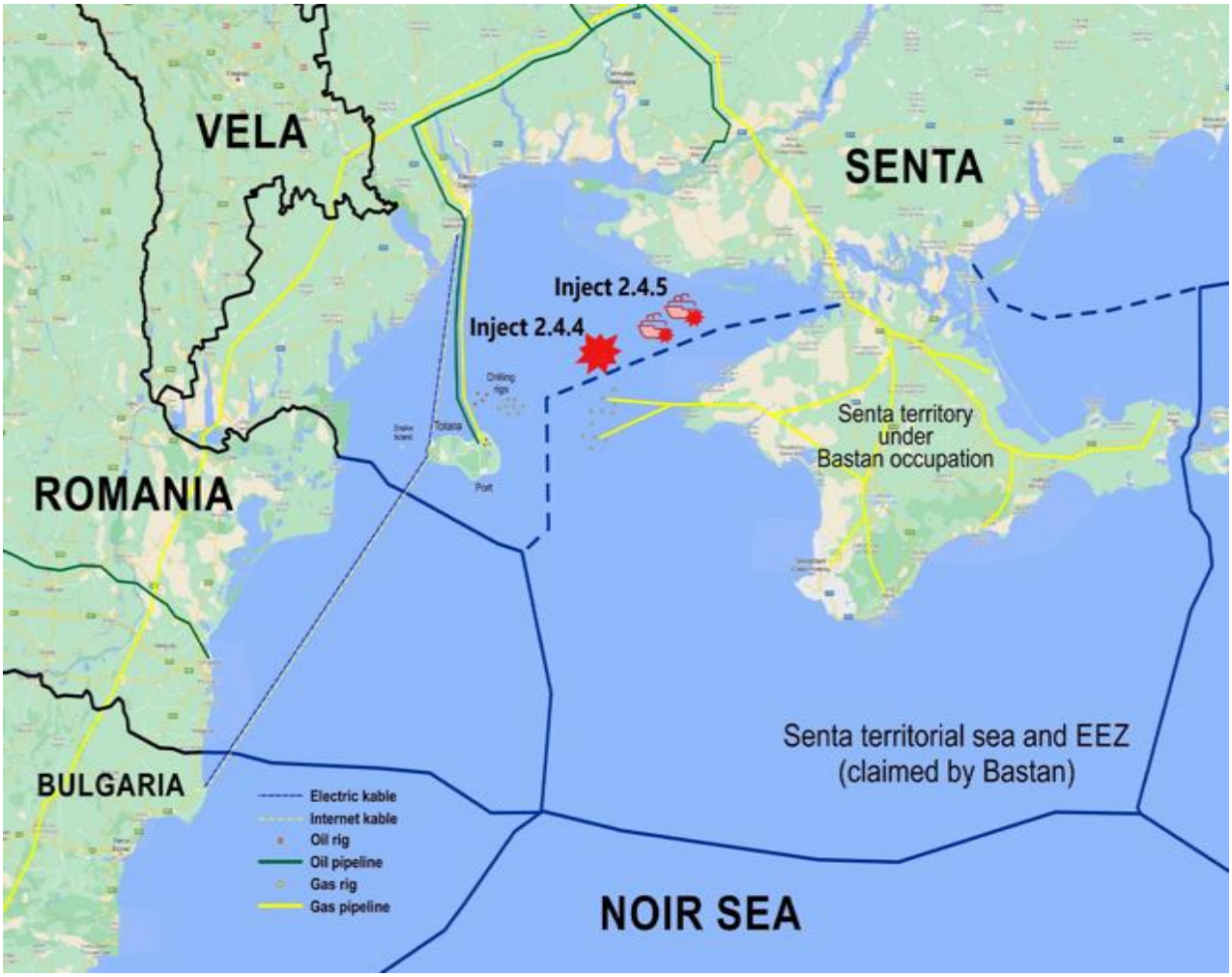
Tanker belonging to Senta suddenly loses control and collides into Bastan's cargo ship in EEZ of Senta, causing the discharge of oil and a significant fire. Some casualties are reported. Bastan accuses Senta's authorities of sabotage. The entire Bastan's media uses this example to underline the necessity of the Bastan Navy to be present in the Noir Sea and defend Bastan's interests.

Response to Inject 2.4.4

The syndicate determined that Ministry of Foreign Affairs and Ministry of Internal Affairs would be the lead here (absent a STRATCOM center) to appeal to allies and partners to strengthen their presence on the Noir Sea in order to ensure the work of the State Emergency Service of Senta in the contested region is not blocked. Additionally, they identified the need for the central government to communicate and coordinate with the local authorities to avoid conflicts. Finding out the reason for the loss of control of the tanker, whether it was the influence of Bastan's Security Service, a possible cyber-attack, or an act of terrorism, and communicate findings to all three audiences. The syndicate singled out the Bastani families of the victims as deserve particular attention when crafting messages to the international community and the aggressor. It was also suggested to get information from the owner of the vessel, through the agency company, as well as the nearest ships (State Border Guard Service, Navy, Marine Guard) to find out the circumstances of the accident, to record what happened, and to ensure coverage in the media. MPRS (utility service) should also update operational information. Reassure the domestic audience that we know about the situation, that we are finding out the situation regarding the dead and providing assistance to all parties. It is also important to send a message about Senta's lack of guilt. For the international audience, it was suggested that these lead agencies also promptly convey truthful information about the Senta's non-breach of its obligations (based on legal expertise).

Inject 2.4.5: Day 48: February 22, 07:00

The Bastan Navy and coast guard intimidate Senta and Zestan civilian cargo ships heading to Senta's ports in the Noir Sea while being in EEZ of Senta and demand their course change back to the outer border of Senta's EEZ. According to Bastan media sources, Senta's civilian cargo ship deliberately attempted to ramp into Bastan's navy ship. The information is later repeated by the Bastan Ministry of Defence, who accuses Senta's ships of provocative and dangerous actions. According to Bastan's media reports, under such circumstances, Bastan's authorities have decided to increase its Naval presence to protect its ships and interests from provocative actions of Senta.



Response to Inject 2.4.5

Here the Ministry of Defense should take the lead, according to the syndicate, to appeal to Senta partners and implore them to strengthen their presence in the Noir Sea. It also should announce that military exercises are commencing. The Ministry of Foreign Affairs should lead an initiative with these partners to convene a meeting of the UN Security Council to address the escalating situation. The primary foreign audiences should be the neighboring countries in the Noir Sea as well as European countries to determine the assistance needed for this crisis. Access to regional formats such as Quadriga should be activated by the MoD and MFA for preparation of joint applications. To reduce the degree of panic among the population, emphasis should be placed on the location of the incident (indicate that it was not in the territorial waters of Senta). The syndicate then spent a significant amount of time discussing processes. They began by trying to define a categorization for crises, and then a matching protocol of actions, and then one of communications. NATO SMEs redirected them to instead focus not on the definitions themselves, but on the elements needed to act together instead of as individuals. This led them to draw conclusions about the need for a centralized structure and processes to guide both crisis response and STRATCOM.

6.3. Vignette 3: Conflict Phase: High-intensity Hybrid Operations

Senta's critical infrastructure experiences a wide range of kinetic and non-kinetic attacks. Disruptions occur on the natural gas transmission pipeline in the Southern gas transit corridor, affecting supply to the Southern region of Senta and the neighbouring foreign states. Moreover, there is a threat of disruption of the heating season not only in the southern part of Senta but in Kharkiv and Luhansk regions as well, in particular those heavily depending on the gas supplies from Bastan.

In the South of Senta, there is a one-third increase of the number of emergencies, fires and accidents caused by arson and terrorist attacks using explosives, which in turn has led to a significant increase in the number of casualties. A significant incident is suspected in PJSC 'Odesa Portside Plant' where the considerable release of hazardous chemicals is reported.

Information on disruptions in the South Senta NPP operation is disseminated. Bastan's media blames Senta's authorities for the release of radiation. Almost at the same time, information about the attack against hydroelectric pumped storage power plant attack is being spread.

Massive cyber-attacks disrupt the operation of the Odesa Sea Port, including transportation and cargo handling. The branches of Oshchadbank and PrivatBank banking systems in the Odesa region were attacked.

In a month after the first cyber-attack on Liebherr's internal network in Germany, there have been a series of minor cyber-attacks on the Liebherr's port cranes all over Europe.

In the maritime domain, Bastan's Navy ships are increasing their presence in the Senta's EEZ, using navy exercises and interrupting the international passenger and cargo sea transhipment.

Inject 3.4.1: Day 53: February 27, 11:00

Two explosions sink two cargo vessels owned by Senta and Zestan, proceeding to Sea Port Pivdennyi. Two buoyant WWII contact mines are detected by surveillance planes and eliminated by the Senta Navy. The government of Zestan releases initial technical evidence compromising the assumption about old contact mines: all damage is located deeper under the hull, near the stern, and all explosions hit the engine room. Some international shipping companies declare Senta's EEZ as dangerous for shipping.

Response to Inject 3.4.1

The syndicate first suggested launching a determination of the level of damage, with changes in the composition of the working group, and bringing in other relevant agencies (SES, Ministry of Health, Ministry of Reintegration). Furthermore, a permanent 24/7 Communication Center is launched, with daily briefings for Ukrainian and international journalists. The syndicate was generally comfortable assembling a new ad hoc group to deal with the current crisis, because that is their experience with past crises, but some members voiced concern that there should be more forethought and policy guiding crisis response, so as the be more efficient and to reduce the time required to react. Social networks, information via leaflets, and civil society in general should also be mobilized. In case of emergencies, the SES should be the lead in this crisis. Alternate communication mediums, such as medium-wave broadcasting and leaflet distribution, should be organized pre-crisis. There needs to be uninterrupted STRATCOM with the domestic population, with all possible mediums mobilized, and be positive and make suggestions as to how to improve the economic situation. For international partners, Senta should be framed as a reliable

partner, who provides truthful information, and who will work hard to clarify the situation as soon as possible. The Government should announce trawling and safe passage in the area of cargo ships and ensure the safety of international ships. This message should be repeated often. Finally, the discreditation of Bastan at the international level can be enabled by Senta's use of positive narrativization.

Inject 3.4.2: Day 54: February 28, 08:00

Major explosions at Ammonia production and storage facilities in PJSC 'Odesa Portside Plant'. Significant release of ammonia and other hazardous chemicals in the atmosphere as a result of an explosion. Dozens of casualties are reported in the plant. The toxic cloud of ammonia is heading towards Odesa city and neighbouring towns.

Bastan media and some of Senta's media report that the incident was staged as a provocation by Senta security services.

Response to Inject 3.4.2

The syndicate determined to establish an operational anti-crisis headquarters, comprised of the SES + CVS + local authorities. Once again, some members were concerned at the number of ad hoc committees or headquarters that were being created to deal with various issues, leading to difficulties in effective coordination and time lost establishing the teams. Within the new crisis team, communication protocols should be employed, with top priority given to gathering information and informing the population. That this was an act of sabotage by Bastan should be the clear message. The MFA should lead on informing external audiences, with the involvement of relevant departments and services of neighboring countries (which may also suffer from some of these consequences) in the MFA headquarters in Kyiv. Protocols such as the introduction of hotlines for the population, the creation a network of regional crisis centers reporting to Kyiv, the creation of a hub of international journalists in the main crisis center, identification of speakers, and the activation of an emergency notification system were all suggested.

Inject 3.4.3: Day 54: February 28, 09:00

Bastan's Navy declares a shooting and exercise area dangerous and blocks a sea route to Odesa Sea Port. An intense LIVEX, including the use of various arms systems, has been ongoing for two weeks and is situated in the vicinity involving merchant vessels navigating through the area - disrupting shipping activities.

Response to Inject 3.4.3

Effects were discussed first: economic losses, international image losses, internal threats, and the national security risk of the occupation of the Noir Sea by Bastan. Objectives were discussed next, with the following narratives suggested: restoring shipping as soon as possible, consolidating international support for Senta, discrediting Bastan and its false narratives, reducing social tensions in the region, restoring and maintaining Senta's international image, and making visible the support of the international community (addressed to both the domestic and Bastan' audiences), building a sense of security and trust of the population. Mechanisms to achieve these goals are primarily led by the Ministry of Foreign Affairs because the need to intensify informational and explanatory work with partners is essential, as well as consulting with Bastan on what can be done to diffuse the situation. The Ministry of Defense should also assist with information operations, informing the public about strengthening their presence in the region. The Regional State Administration should enact meetings with businesses and call for continued payment of salaries and price stability at the level of the Prime Minister.

Inject 3.4.4: Day 55: March 1, 12:00

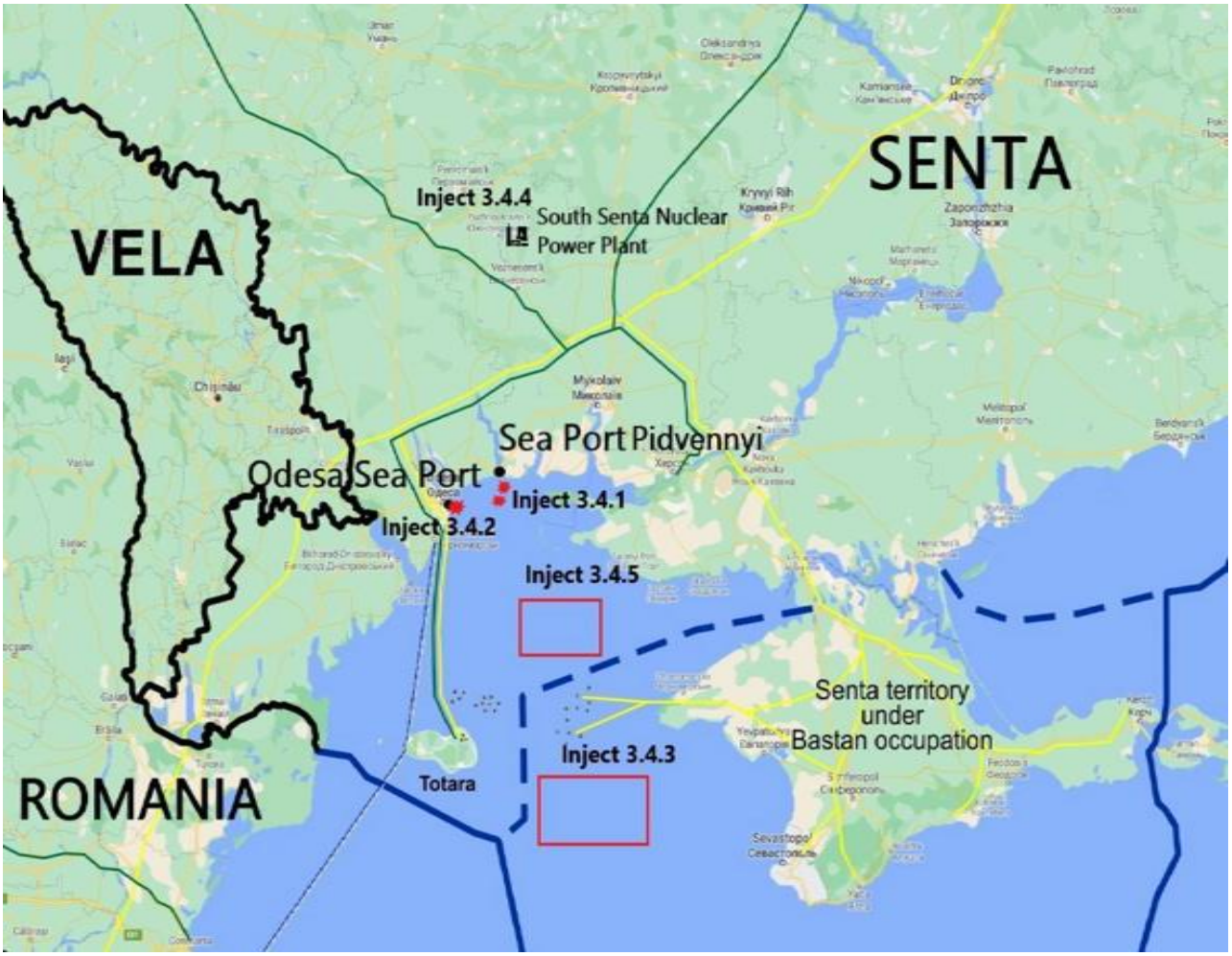
False information about the emergency shutdown of the South Senta NPP is being disseminated. Bastan media blames US nuclear fuel suppliers and Senta's 'corrupt power' while spreading reports of a large-scale incident at a nuclear power plant with significant radiation release. Some of Senta's eco-activists accuse Senta's authorities of lying about the incident. Based on information from Bastan, international TV channels along with some media of Senta are spreading the message about the possibility of a new 'Chernobyl'.

Response to Inject 3.4.4

Because effects of this spreading narrative have potential to create panic in the country, even destabilization, an economic downturn, a refugee risk, and panic among partners of Senta, reassuring the domestic audience should be the top priority. The MFA should lead in providing truthful information about misinformation, demonstration of Senta's subjectivity, should involve US partners to help clarify, and should call in international journalists. The State Agency for Nuclear Safety should come out and refute the information forcefully, and even invite IAEA representatives. For internal audiences, there should be a response from the Center for Counteracting Disinformation of the National Security and Defense Council to address the fake narratives in order to calm the population and prevent panic. Some mechanisms discussed were press tours for journalists, outreach to the public, communication in advance on the protection of other nuclear power plants, sufficient fuel, radiation measurement points, and informing the population about the actions of Bastan.

Inject 3.4.5: Day 56: March 2, 16:00

Bastan establishes a control zone where ships bound to Senta are stopped and searched by Bastan's Navy, the coast guard, or both. The motivation for these acts, as announced by Bastan, is a suspected terrorist threat against undefined strategic targets. Ships are subjected to random controls. Delays are ranging from five hours to two days. The average waiting time per vessel is 20 hours.



Response to Inject 3.4.5

Effects were discussed first: economic crisis is becoming worse, the image losses of Senta in the international arena is growing, there are growing social tensions, and there is a very real likelihood of escalation with Bastan. Objectives were discussed next: to restore shipping, to reassure international partners, and to reduce social tensions. Steps to these objectives: STRATCOM narratives via the MFA for the international audience (including partners and Bastan), proving to partners the situation that has arisen is based on false pretenses and that Bastan is violating international law, and providing a positive narrative telling Senta's side of the story. These narratives should also be incorporated and issued by the MoD and Regional State Administration.

6.4. Vignette 4: Hybrid Warfare

Tensions between Bastan and Senta have reached the highest level ever. Senta's military intelligence reported an unprecedented number of military build-up in Bastan Navy's bases in the Noir Sea. A significant number of provocative accidents have started to occur on Totara Island. Reports of the loss of GPS and GSM signals on the island. The Internet connection on the island was disrupted.

At the same time, Senta continues to experience a growing number of cyber-attacks against governmental and local institutions, and critical service providers. Bastan's and Senta's media aggressively reports about the inability of Senta's central and local authorities to provide critical services for the population. Moreover, top commanders of Senta's armed forces in Kyiv and Navy officials in Odesa and Totara Island received e-mails from unconfirmed accounts with a direct warning 'not to follow orders of Senta's political authorities, or they and their families will be in danger'.

Social media is full of reports and active discussions about the possible separation of the South part of Senta. The same news is being spread via official web pages of regional councils. The above leads to pressure and tensions inside governmental institutions, law enforcement agencies, and armed forces. In the last 24 hours, street manifestations against the Senta government intensified dramatically, namely in the central cities of southern regions: Odesa, Mykolaiv and Kherson. As a result, the government is overstretched, and the population is confused.

Against the background of significant cyber disruptions, psychological pressure, the spread of misinformation, and growing street manifestations in southern regions, suddenly a considerable number of military forces without insignia launched on the Totara Island. The access to the Port of Totara Island is blocked by the cargo ships with no State flag identification. The access by water to the Totara Island is cut off.

The drilling rigs for hydrocarbon production of Totara Island located in the Senta's EEZ were occupied and now are under the full control of armed men with no State identification.

Inject 4.4.1: Day 56: March 2, 05:00

Armed men occupy eight gas rigs off Totara Island in the EEZ of Senta without insignia who used helicopters to land on the rigs and took them over. Bastan's Navy establishes a control zone around rigs, namely in Shtormov and Halitsyno gas deposit areas. Civilian ships and aeroplanes report significant disruptions of GPS signals in the Noir Sea region.

Response to Inject 4.4.1

The effects of the crisis are discussed: loss of critical infrastructure, deepening economic crisis, airspace and sea-lane closure, and growing social tensions. The objectives the syndicate decided on include a call for all international partners to increase their presence in the area and to unify the country against the actor responsible for the situation: Bastan. A target audience analysis was then discussed: who can be a partner in deescalating the crisis, who can provide information support to get the messaging to the different audiences, who can provide verbal support for Senta, who will not comment on the situation, and who will oppose Senta. In the meantime, there should be preparation of messages for de-escalation of the current crisis, how to announce the successful completion of the operation, with the possible simultaneous statement from the President together with partners. There should be tight security of operations during all actions and events, with simultaneous coverage of what is happening in the information space, including international and adversarial.

The SBU should conduct an anti-terrorist operation and be the lead on this crisis. Auxiliary support should be structured as follows:

1. Meeting of the National Security and Defense Council

2. MFA: Initiative to involve international organizations.

3. Territorial defense meetings - in all regions, to unify Senta against Bastan.

4. Preventive measures so that Bastan does not show themselves as the victim.

5. Ministry of Foreign Affairs should determine the countries that will support and those that will not to create different messages for different international audiences. It should also create a coalition of states that will support Senta, highlighting support in the information space with joint bilateral and multilateral statements.

6. Ministry of Defense should launch information operations to support the population in Totara Island, including the military there.

7. Internal audience – all Senta servicemen and their relatives should be reassured.

8. Intelligence of foreign partners should help with the identification of Bastan's involvement.

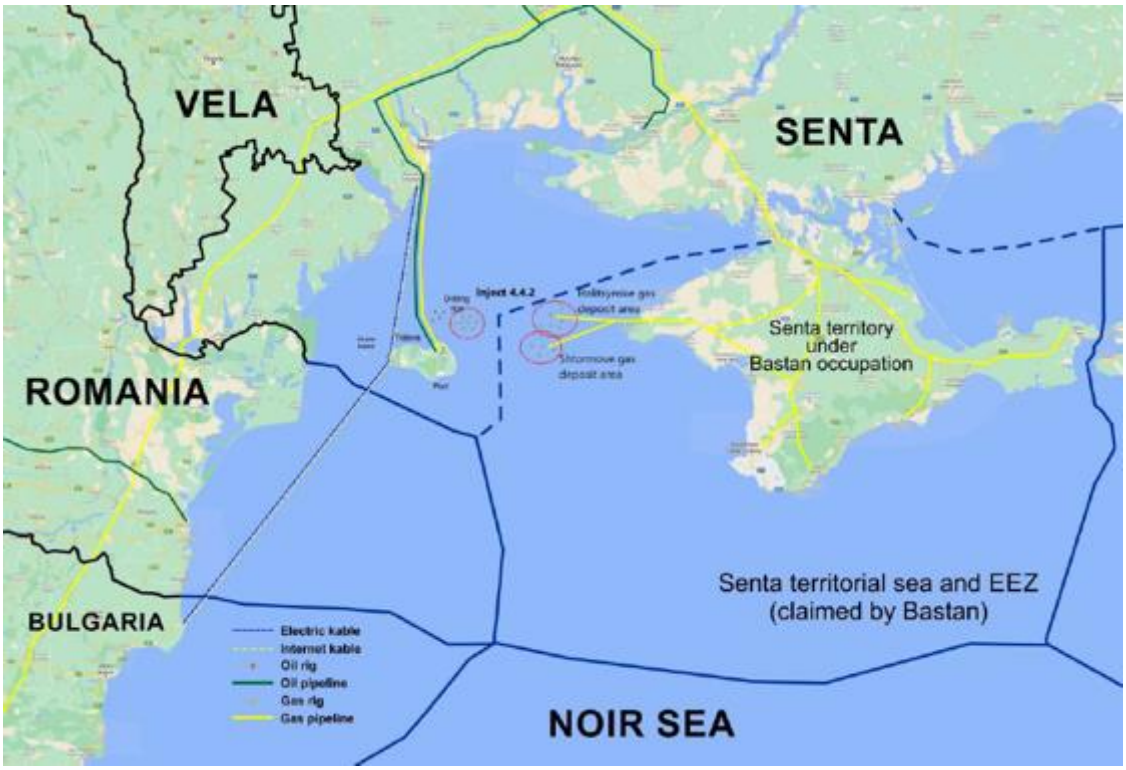
9. Involvement of the public via training of actions in emergency situations, public safety, etc., short videos on social networks highlighting the truth of the situation on Totara Island. The local population should receive instructions on first aid and the detection of dangerous objects.

Inject 4.4.2: Day 58: March 4, 02:00

A significant number of heavily armed men without insignia land on Totara Island.

Reports about the takeover of local institutions and major Senta's naval base on the island. Bastan's authorities deny any involvement in the operation. TV media of Bastan accuses Senta's far-right forces of genocide against the local population. No Internet and GSM coverage is now available on the island.

At the same time, the website of Totara's parliament declares that to protect the local population from genocide by far-right forces of Senta, the island's authorities decide to declare secession from Senta and appeals to Bastan for help.



Response to Inject 4.4.2

Effects were again discussed first: the continued violation of the territorial integrity of Senta, the destabilization and social tensions, the likelihood of open military conflict, the worsening economic crisis, the complete blocking of maritime traffic, and the threat of loss of international support, all as a result of Bastan's hybrid actions. The importance of communication cannot be understated here. Objectives were then discussed: restoration of territorial integrity, prosecution of Bastan for their international law violations, and the restoration of Senta's image in the international arena. The primary external audiences include the diaspora (World Congress of Ukrainians) and the UN (official notification of the right to use force). For internal audiences, priority is given to the Armed Forces on Totara Island and the rest of the territory, their relatives, as well as neutral, pro-Bastan, and Protestant populations. The involvement of churches and religious organizations to inform society is also suggested. The messaging based on the audiences should be varying degrees of: we have the right to use force, it is not a civil war, it is external aggression by Bastan, and there is no genocide on Totara Island.

6.5. Vignette 5: Post-Crisis Stablisation

The present vignette focuses on the post-crisis and recovery stabilisation process. The post-crisis stabilisation takes place after the end of the crisis scenario – from March 7, 20YY. Crisis management issues are to be discussed, as well.

Each syndicate will be presented with several questions for the post-crisis stabilisation discussion.

1. Is there an effective system of strategy, including crisis, communications? How do you ensure effective and credible strategic communication with the outside world? What are the main issues/challenges in the area of strategic communications?
2. What are the ways to improve the existing system? Does it require additional elements that are currently missing?
3. How would you detect, analyse and counter disinformation campaigns for internal and external audiences?
4. How do you see the ways of the public and private sector's engagement in strategic communications systems?

Syndicate did not complete Vignette 5.

6.6. Key Takeaways

Create a STRATCOM office at the ministerial level. From a STRATCOM perspective, Ukraine knows the adversary very well and knows how Russia conducts hybrid operations. However, it does not have the protocols, institutions, and mechanisms to respond in a timely, coordinated, and efficient manner. Many participants acknowledged that there is an absence of: 1) clear leadership to coordinate the efforts of STRATCOM elements which exist in various organizations, 2) interagency communication and coordination, and 3) private sector-government communication and coordination mechanisms. This absence hinders effective crisis response at the strategic level. There is no clear high-level (ministerial) function to organize the disparate groups to create a unified communications strategy, or to align the efforts of each group to support that overall strategy. As a result, they need to create an ad hoc team for each crisis, which is slow and inefficient. In terms of STRATCOM response narratives, speed and agility in messaging is perhaps the most important part of achieving their objectives. **Recommendation(s):** Create a STRATCOM office at the ministerial level with clear and unified leadership that works as consolidation agency to produce streamlined narratives for domestic, international, and adversarial audiences. The syndicate recommended a ministerial-level independent national crisis communications position directly under the prime minister. Recommend implementing this position and making it a permanent, continuous agency, not an ad hoc team that is only created to coordinate each crisis that arises.

Improve and build STRATCOM protocols and procedures for rapid and coherent responses to crises. National crisis management plans, policies, and procedures to respond to and to mitigate the effects and impacts of hybrid actions is perhaps the most lacking aspect of Ukraine's current STRATCOM structure. Ukraine does not currently have baseline protocols or mechanisms to rapidly respond to hybrid threats. In addition to not having a single point of leadership and coordination as mentioned above, they are currently inefficient at both determining the level and type of response needed and at producing narratives for different relevant audiences when hybrid crises arise. The syndicate noted the lack of or inadequacy of mechanisms of coordination between institutions, the lack of definitions for crisis

classification levels, an insufficient number of state channels of communication with the population, and the lack of any kind of pre-determined public notification system. Power outages, transportation disruptions, denial of service attacks, flooding of disinformation on social media and Russian state mediums, and targeted threats to individual citizens via digital technologies have all been part of Russian hybrid actions against Ukraine. If a crisis ever evolves into hybrid war, Russia will certainly utilize all if its capabilities to disrupt and degrade communications to further sow chaos and confusion among the Ukrainian government and population. STRATCOM must be prepared for these disruptions and have contingency plans in place to get their messaging out under these circumstances. **Recommendation(s):** Develop protocols and an organization and codify them in government policies/laws, so that it will not be necessary to create them in a crisis. Include a classification for types of crises by severity and by which government and private entities need to be engaged, as well as defined levels of response that include who would deliver the message and through which channels. Standard procedures and pre-approved protocols could reduce response times, allowing leaders to further understand the situation. Put risk assessment protocols in place, so that the various audiences are able to understand the seriousness of the crisis and how it affects them. Put crisis communications protocols in place to be able to communicate via land line telephone, radio, mail, and even leaflets in order to reach audiences under extreme circumstances. These contingency plans are crucial to prevent unrest and panic amongst the populations if a hybrid warfare scenario occurs.

Develop a standard method of planning STRATCOM, including strategic narratives regarding domestic, international, and adversarial narratives. Ukrainian elements have a clear understanding of tactical-level messaging, but no overarching frameworks to guide the effort of messaging during a crisis. Each organization has their own standard methods of planning and targeting STRATCOM, with no clear organizational level division of messaging, such as for the target audience (domestic/international/adversarial). They need to decide what outcome they want, which narratives to develop for each target audience, what effects they expect, and how to execute them in a timely manner. Even after clear protocols have been established under a ministerial-level communications director, there will still be a need to quickly develop and disseminate messages that are consistent with strategic themes. **Recommendation(s):** Create a model that ensures a common method for planning and disseminating strategic communications (e.g., desired outcome, target audience, expected effects, and execution). Specifically, STRATCOM elements need to frame their efforts into some variation of the "Activity->Audience->Message->Perception->Desired Outcome" model. Develop pre-approved messaging themes based on defined crisis levels that can quickly be released when needed. What do they tell their various domestic audiences? How do they communicate to their Western allies and partners? What measures should be taken to mitigate the narrative coming from the adversary? These are questions that should be asked before every public messaging campaign, and in order to collaborate across the various organizations involved, they must have a common method of approach.

Plan ahead, and always be at the strategic level. National crisis management plans, policies, and procedures to respond to and to mitigate the effects and impacts of hybrid actions is perhaps the most lacking aspect of Ukraine's current STRATCOM structure. Ukraine does not currently have baseline protocols or mechanisms to rapidly respond to hybrid threats. In addition to not having a single point of leadership and coordination as mentioned above, they are currently inefficient at both determining the level and type of response needed and at producing narratives for different relevant audiences when hybrid crises arise. The syndicate noted the lack of or inadequacy of mechanisms of coordination between institutions, the lack of definitions for crisis classification levels, an insufficient number of state channels of communication with the population, and the lack of any kind of pre-determined public notification system. Power outages, transportation disruptions, denial of service attacks, flooding of disinformation on

social media and Russian state mediums, and targeted threats to individual citizens via digital technologies have all been part of Russian hybrid actions against Ukraine. If a crisis ever evolves into hybrid war, Russia will certainly utilize all if its capabilities to disrupt and degrade communications to further sow chaos and confusion among the Ukrainian government and population. STRATCOM must be prepared for these disruptions and have contingency plans in place to get their messaging out under these circumstances.

Recommendation(s): Develop protocols and an organization and codify them in government policies/laws, so that it will not be necessary to create them in a crisis. Include a classification for types of crises by severity and by which government and private entities need to be engaged, as well as defined levels of response that include who would deliver the message and through which channels. Standard procedures and pre-approved protocols could reduce response times, allowing leaders to further understand the situation. Put risk assessment protocols in place, so that the various audiences are able to understand the seriousness of the crisis and how it affects them. Put crisis communications protocols in place to be able to communicate via land line telephone, radio, mail, and even leaflets in order to reach audiences under extreme circumstances. These contingency plans are crucial to prevent unrest and panic amongst the populations if a hybrid warfare scenario occurs.

7. Syndicate 5: International Response/International Law

The International Law syndicate discusses "key takeaways" identified through the execution of the CORE 20 TTX in Odesa, Ukraine.

7.1. Vignette 1: Pre-conflict Phase: Hybrid Influencing

Political and economic intimidation against Senta by Bastan authorities is growing. On the basis of the gas transit agreement, which has been signed by Bastan and Senta last year, the Bastan government accused Senta of infringing agreement provisions. Senta denies any violations. However, Bastan's media and some Senta's media controlled by Bastan keep spreading the messages about Senta's violation, stressing the importance of the corresponding agreement for Europe's energy security as the gas transit to European countries is partially ensured through the territory of Senta.

The situation is aggravated by the fact that there is no new contract for gas supply between Bastan and Vela. Given disputes over contractual provisions, Bastan temporarily substantially reduces gas supplies to Vela. Vela maximally draws gas from the transit pipeline, limiting gas supplies to Senta's customers in the Odesa region, near the border with Romania.

Meanwhile, Bastan inflicted import restrictions on Senta's agriculture, manufacture, and metal products, as well as fuel, chemicals, and petroleum products. Besides, Bastan ceases to supply oil products to Senta with automotive, railway transport, and pipelines.

Three websites were found on the Internet with identical visual designs and features of the official websites of Senta GTS Operator, PSG Operator, and Naftogaz Company. Moreover, e-mails with phishing features and attached Microsoft Word text documents have been found in the e-mail boxes of Senta's regional government agencies.

Media reports were released about the powerful cyber-attack on Liebherr's internal network in Germany. As a result, port cranes at the Poti Sea Port in Zestan have stopped working.

From the middle of December, Senta's coast guards are regularly reporting about the Bastan's Navy presence in the Senta's EEZ. It is reported that Bastan conducted military exercises in the Noir Sea in the nearest vicinity of the fairway passage of merchant and passenger ships from/to ports in the Odesa region.

Inject 1.5.1: Day 1: January 6, 11:00

A year after signing the gas transit agreement, Bastan authorities accuse Senta of violating the agreement – warning to terminate the contract and halt gas supplies through Senta's territory.

Response to Inject 1.5.1

The question was brought up regarding whether signing an agreement that has not yet been ratified would make it legally binding or not, it was decided to assume it to be legally binding for the scenario. Senta needs to understand what parts of the agreements they are accused by Bastan of breaking, which necessitates the Gas companies and Government of Senta being able to quickly and efficiently communicate. The situation is complicated because there are two parties involved in this, commercial gas companies and Senta's Government, specifically Minister of Foreign Affairs (MFA) and Minister of Energy (MOE). Natural Gas companies should respond to these accusations, but since they are a commercial company, the government must also ensure that a clear unified message is put out to the populous and the international community. The other issue is that gas is simply transited through Senta to other states (specifically EU countries). These other countries' gas providers will have the ability to also show if they are in fact seeing issues or not, which makes getting information out to the international community an even more important issue. Senta must not allow Bastan to drive the informational picture, particularly if this information is false. It is important that any information put out by Senta in the commercial or governmental area must show that business is being done as required and that obligations are in fact being kept, and this should be simply informational and not reactionary, Senta must show its neighbors that it is competent and reliable.

Recommendation: The ability to react and method of reaction must be a part of policy. This policy needs to be created before incidents occur and be clearly understood by critical infrastructure providers as well as the government of Senta. These critical infrastructure parties (gas companies in this instance) should be involved in the creation of this plan to ensure its effectiveness when utilized in a time of need. A public-private coordination body (led by Ministry of Foreign Affairs or Ministry of Information Policy) should be set up as a pre-crisis center in Senta government to react quickly, to reduce reaction time from a week to just hours.

Recommendation: It is important to ensure that press releases and statements are put out and posted online by Senta in not only Ukrainian, but English and other languages of international nations. Particularly English version would be helpful to ensure that the international community can immediately understand and be made aware of the situation. When information is put out in Ukrainian only, it prevents a quick international response from being possible, hindering the assistance that Senta might otherwise receive, due to translation delays. Syndicate team says, "an English version of news can be put out to google and from there it will spread quickly to everyone."

Recommendation: National Action Plan for Gas Supply of Senta needs to be updated each year. Enable EU countries to make purchases of gas directly from the Senta – Bastan border to demonstrate Senta as a reliable provider of gas and minimize transit risks.

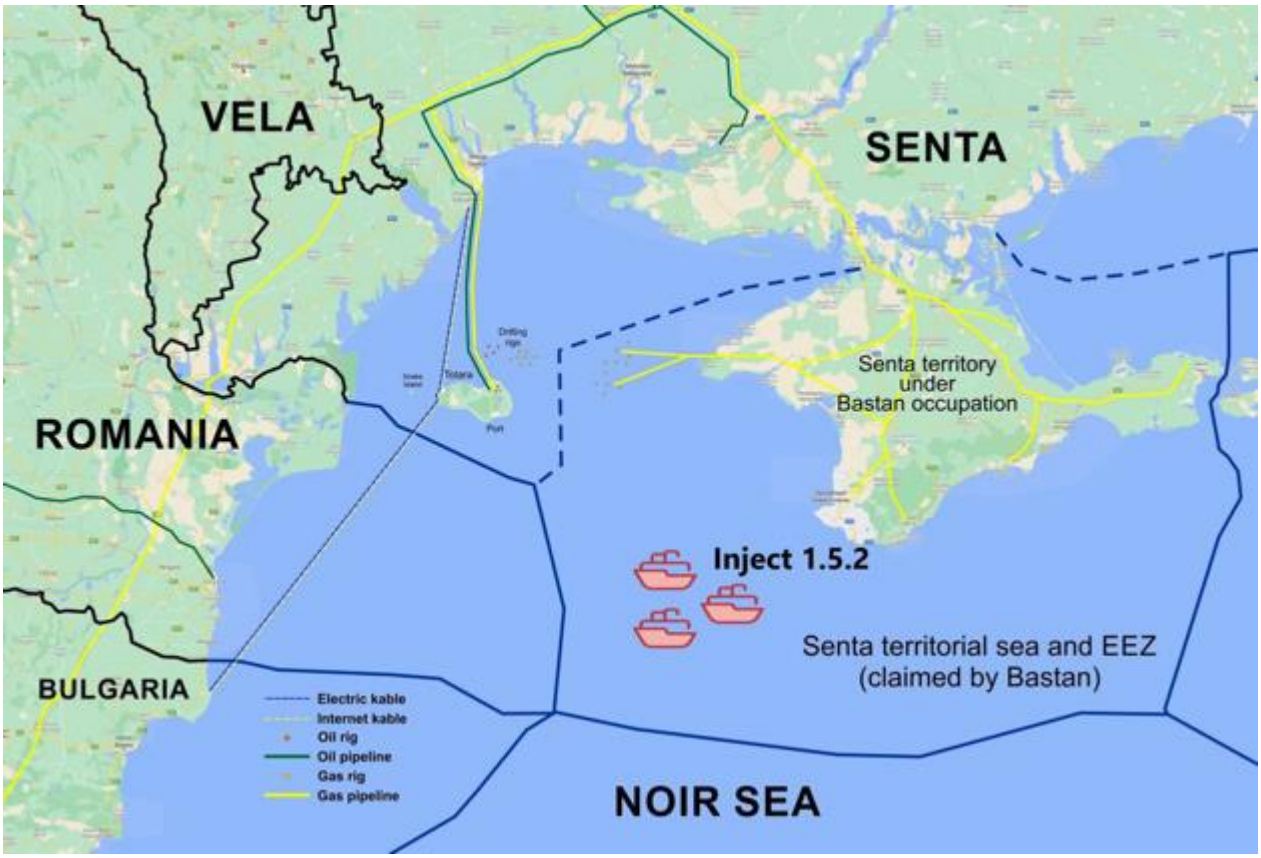
Recommendation: Providing informational response to accusations should be immediate and not delayed waiting to acquire all the facts before responding. This becomes a time delay that is detrimental for Senta. A quick reaction to inform the international community on the situation as Senta knows it now must be put out and further amplifying information can be provided afterward. Waiting to determine all the facts and saying nothing, gives Bastan's dialog more weight, even if untrue. Even in all facts are not known, and further investigation is necessary, Senta can put out statement based on principles (e.g., debts will be honored, contracts will be followed, full & open investigation will follow, etc.)

Recommendation: Border state quick reaction teams should be established to ensure a quick response when there is a threat to security or peace, in order to minimize threats. Currently many border state agreements involve meetings that happen only a few times a year. There is a need for a standing method of quick communication between border states to react to crisis situations.

Recommendation: Ensure Presidential Security Council can operate in accordance with Presidential decree #115, issued Feb 28, 2015, as the primary lead to identify crisis situation and create a Crisis Center with Secretary of Security Council in charge of stand-up.

Inject 1.5.2: Day 5: January 10, 10:00

Bastan Navy is present in Senta's EEZ with ships not responding to informational requests by Senta's coast guards. Bastan Navy ships are also harassing commercial shipping transiting to Odesa Sea Port under the pretext of "conducting a security operation."



Response to Inject 1.5.2

Senta must react every time these laws are breached, even if it is all the time. Partner countries must be asked for help in patrolling and ensuring the opinions of partner nations are correct, Senta must not let Bastan control the information seen by partner nations. Involving partner nations will ensure they can also provide information to show what is going on in the Noir Sea. Bastan is stopping ships in the EEZ of Senta, this is not allowed. Joint patrolling of the EEZ is vital. When a breach of state borders occurs, the security council must be involved and make further recommendations. The security council does not provide direction to the Presidential Branch, it is questioned if there is a clear plan of what should be done when an EEZ breach is taking place. There is a civil defense code, but it is outdated (created during the Ponuxin Empire), but it provides emergency responses.

Recommendation: Updating the Civil Defence Code is necessary and can provide an internal reaction plan to threats. This needs to be updated with crisis scenarios to ensure a national response plan. Particularly developing specific crisis scenario responses for violations of the EEZ from the sea.

Recommendation: Important that commercial shipping harassment is addressed as a state security issue, not a commercial legal dispute. Ministry of Foreign Affairs should ensure commercial contracts regarding shipping are direct and clear on right of Senta government to intervene.

Recommendation: Ensure there is a tested and effective mechanism to inform international partners (NATO and bordering maritime partners) directly and immediately of these types of disputes. Old Soviet era friendship/partnership agreements with bordering nations could be updated and used to create consultation and assistance mechanisms. Thereafter agreements could be re-examined annually.

Recommendation: Senta should standardize its ability to reach out to NATO under Paragraph 15 of its partnership agreement with NATO without hesitation when territorial integrity issues emerge. Emergency meetings with NATO should not be at question. Senta should consistently use Paragraph 15.

Recommendation: Senta should create maritime patrolling agreements and ability with its maritime neighbors to enable multilateral response in these types of situations. Coalition coastal patrols need to become routine before the crisis occurs. Senta should pursue such agreements ASAP.

Recommendation: Senta should organize exchange/fellowship opportunities between Senta and NATO/EU countries to exchange ideas and learn about issues involved with hybrid warfare before conflicts develop.

7.2. Vignette 2: Low-intensity Hybrid Operations

Weather conditions in the Southern regions of Senta deteriorated at the beginning of February. Wind speed reaches 50 m/s index causing considerable damage, namely in the Odesa region.

Bastan's import restrictions on Senta's agriculture, manufacture and metal products, as well as fuel, chemicals and petroleum products contribute to the decline of Senta's economy which has already been in recession. Pro-Bastan activists use the economic downturn as a chance to intensify protests against Senta's government. Social tensions reached their peak when news about Odesa City Council's decision concerning secession of the Odesa region from Senta has spread via the Internet.

The work of Odesa Sea Port is continuously disrupted by the actions of pro-Bastan activists and incidents in the cyber-security domain. Moreover, Senta's civilian and coast guard vessels reported technical issues in their navigating system.

Furthermore, Bastan's vessels act aggressively against Senta's fishing boats. Coast guard ships of Bastan intimidate and threaten cargo vessels of Senta and foreign states as well. Recently, Bastan Naval Forces provided support to the illegal gas exploration and drilling rigs installation operation within the territory of Senta's EEZ. The 24-hour security guard patrol of Bastan's Navy was established around the rigs.

Inject 2.5.1: Day 43: February 17, 10:00

Due to severe weather conditions, namely strong wind with corresponding speed of 50m/s, a tanker belonging to Senta suddenly loses control and collides into Bastan's cargo ship in EEZ of Senta, causing the discharge of oil and a significant fire. Some casualties are reported. Bastan accuses Senta authorities of sabotage.

Response to Inject 2.5.1

There is a protocol on pollution of the Noir Sea. Senta should ask NATO countries and countries in the Noir Sea for assistance with the spill. A high-level format of a quick response center is not operational. Need a working group that deals only with emergencies that consists of several ministries to be able to act. Likely that the Ministry of Environmental Protection & Natural Resources of Senta (MEPNR) and the Ministry of Infrastructure of Senta would take the lead. However, if designated as a crisis MEPNR would lose that lead agency designation.

Recommendation: Establish a mechanism for informational requests from Senta's agencies to the Minister of Foreign Affairs on their needs from international organizations. This will provide better coordination and should be established in order to quickly enable MFA to understand exactly what would help Senta's agencies the most, so that MFA can get assistance form the international community quickly and ensure it is the type of help that is most needed. Getting clear information out to international media on hostile behavior is very important, do not allow Bastan's narrative to go unanswered.

Recommendation: MFA should ensure it has effective and rapid communications capabilities with Senta and international think tanks to improve the disbursement of its communications and messaging. Further, Senta should conduct thorough studies with multiple think tanks to develop probable scenarios and response plans for these types of Vignettes (applies to Vignette 2/3/4/5).

Recommendation: Again, Senta should standardize its ability to reach out to NATO under Paragraph 15 of its partnership agreement with NATO without hesitation when territorial integrity issues emerge. Emergency meetings with NATO should not be a difficult question, but rather Senta should err on the side of using Paragraph 15. Requests for joint patrol with NATO should be standardized.

Recommendation: Reconsider which Senta agency has leadership designation over an event that is not a "pure emergency" but is a pressing concern with quick, coordinated actions required. MEPNR may not be the best choice.

Recommendation: Senta should strengthen intelligence/reconnaissance agency capabilities and strengthen interaction with EU and NATO in intelligence issues. Senta should seek to significantly improve the effectiveness of its intelligence work.

Inject 2.5.2: Day 46: February 20, 17:00

Senta's coastal guard ships inform about Bastan actions in the Noir Sea. During the recent time, Bastan has installed gas jack-up drilling rigs, carrying out gas exploration and extraction within the territory of Senta's continental shelf. Bastan's navy ships are patrolling around gas rigs.

Response to Inject 2.5.2

The Security Council must be called and submit an appeal to international laws for Bastan doing drill rigs in EEZ of Senta. Bastan is claiming they have the right based on the illegal taking of Senta's land as theirs, which is not recognized by the international community as legal. So therefore, Bastan has no right to claim they are protecting their own economic interests. The Noir Sea Convention has bilateral responsibilities. Senta should consult with their partners and use their viewing of actions in the private and public sector to point out what Bastan is doing and the issues they are creating in harassing commercial shipping in Senta's EEZ. The real goal is to ensure Senta gets help for trouble with a hostile state's actions. Gathering of information is critical, the executive power can ensure all information is shared with the security council. There is a special way to make an appeal to the international court for this issue as well. Oil spillage is a threat to the whole region, so for this issue, Senta should announce an international meeting to inform country representatives who can assist in a decision for clean-up, this would even include Bastan. Regarding Bastan making jack up rigs in Senta's EEZ, there is a need to establish legal background for rules that do not allow other states to install jack up rigs. We need to have such legal grounds, by not allowing Bastan to continue this, but rather to ensure Senta shows that this is not legal and that Bastan does not have permission to do this in Senta's EEZ.

Recommendation: The international community must be involved and aware of what is going on and the truth of Bastan's blatant violation of Senta's EEZ. The Office of Security and Cooperation in Europe (OSCE) is suggested.

Recommendation: Make continuous appeals to the international courts for the violations. This will keep this fact in the forefront of the international community. It also assists in establishing a desired law violation trend that what Bastan is doing is not legal. Ensure Senta procedures for rapid filings in international courts are clear and known within Senta government.

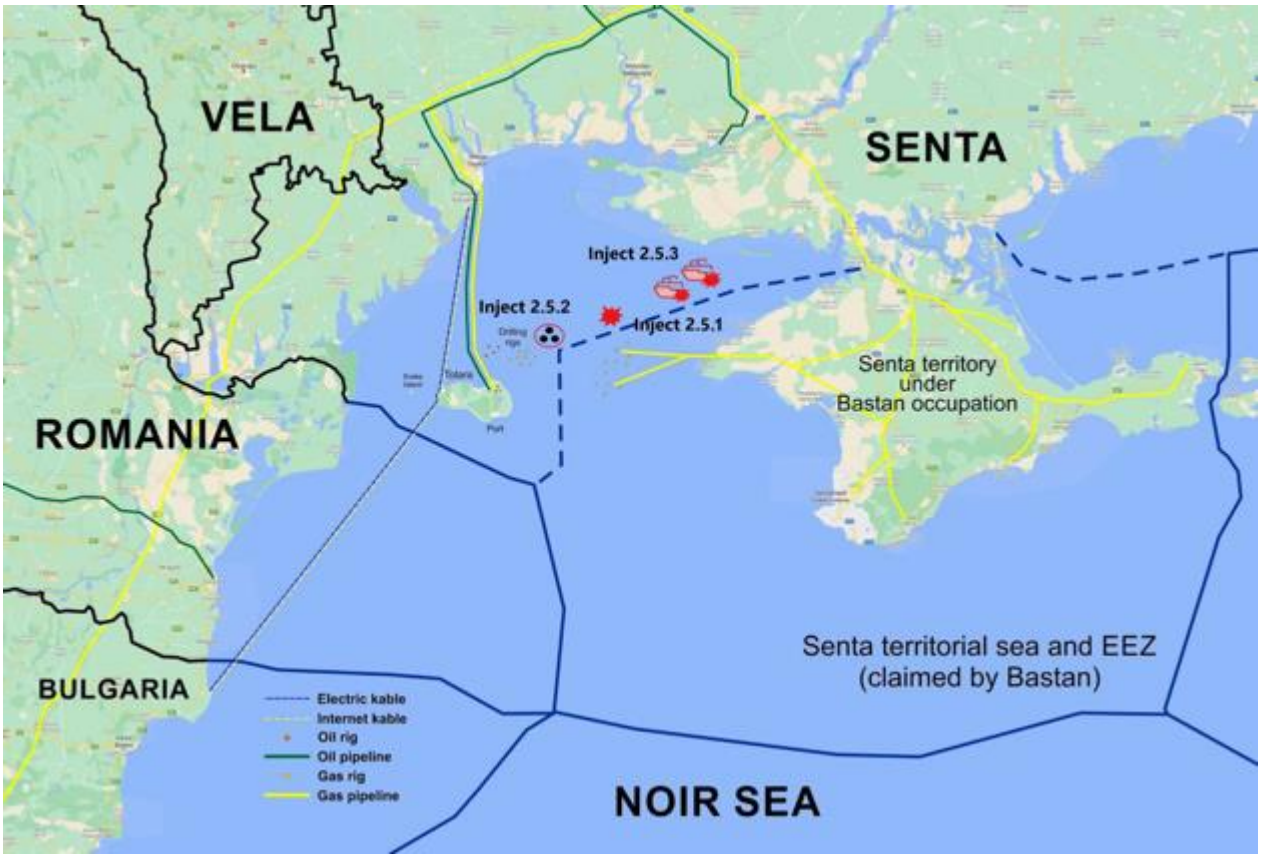
Recommendation: The environmental and trade impacts of aggression to the international community should be voiced. It should be ensured that it is understood that not only is a military action happening against Senta by Bastan, but that Bastan's actions are also impacting the environment and trade, the economic impact affects more than only Senta. Drastic ecological harms must be publicized to ensure international sympathy.

Recommendation: Senta, European partners and NATO Allies should consider how sanctions and threat of sanctions could be used effectively in these types of situations.

Recommendation: Senta should be engaged in a detailed examination of the European Union's civil protection policies documents to understand what it can realistically expect from the EU in these types of situations.

Inject 2.5.3: Day 48: February 22, 07:00

The Bastan Navy and coast guard intimidate Senta and Zestan civilian cargo ships heading to Senta's ports in the Noir Sea while being in EEZ of Senta and demand their course change back to the outer border of Senta's EEZ. According to Bastan media sources, Senta's civilian cargo ship deliberately attempted to ramp into Bastan's Navy ship. The information is repeated by the Bastan Ministry of Defence, who accused Senta's ships of provocative and dangerous actions. According to Bastan's media reports, under such circumstances, Bastan's authorities have decided to increase its naval presence to protect its ships and interests from provocative actions of Senta.



Response to Inject 2.5.3

Media is suggested to be used to help Senta's case. Bastan should be accused of piracy for disrupting commercial shipping. The Ministry of Defense must prepare a press release and all experts must attempt to clarify what happened by fact checking. Bastan's media should not be trusted. Senta border control must state what happened. It is questioned if the EEZ is under responsibility and fiscal control of border control. Senta Navy should be able to establish defined shipping lanes, currently they have not done this. Asking Türkiye for help and appealing to the international maritime organization must happen. The Ministry of Infrastructure must be involved given it involves commercial ships, along with coordination with Ministry of Foreign Affairs and Ministry of Defense.

Recommendation: Development of more clear decrees to define other internal methods to the Senta government to collect, analyze and get information out to the international community quickly. Rapid and

full internal information exchange is vital and procedures should be set ahead of time so response can be within hours if not less.

Recommendation: Negotiation and development of joint action plans with partner countries and neighboring state on actions to be taken in such crisis actions should be developed, with deterrence measure and aids already determined.

Recommendation: Clarify international and domestic laws on piracy. Consider proactive updates to Senta domestic law to ensure this type of interference with shipping is considered piracy. May not be possible if the hostile vessels are under a Bastan flag.

Recommendation: Improve technical ability for intelligence information exchange with regional maritime partners through the Enhance Opportunities Partnership.

Recommendation: Invite military ships of NATO to participate in exercises in the Noir Sea, so that there are other international partners presence there to assist in deterring Bastan's aggressive tactics. Potentially also to invite international partners to assist in ensuring safety of shipping lanes for commercial vessels entering Odesa Sea Port. Perhaps a set system for "Snap Exercises" with NATO could be established.

7.3. Vignette 3: Conflict Phase: High-intensity Hybrid Operations

Senta's critical infrastructure experiences a wide range of kinetic and non-kinetic attacks. Disruptions occur on the natural gas transmission pipeline in the Southern gas transit corridor, affecting supply to the Southern region of Senta and neighbouring foreign states. Moreover, there is a threat of disruption of the heating season not only in the southern part of Senta but in Kharkiv and Luhansk regions as well, in particular those heavily depending on the gas supplies from Bastan.

In the South of Senta, there is a one-third increase of the number of emergencies, fires and accidents caused by arson and terrorist attacks using explosives, which in turn has led to a significant increase in the number of casualties. A significant incident is suspected in PJSC 'Odesa Portside Plant' where the considerable release of hazardous chemicals is reported.

Information on disruptions in the South Senta NPP operation is disseminated. Bastan's media blames Senta's authorities for the release of radiation. Almost at the same time, information about the attack against hydroelectric pumped storage power plant attack is being spread.

Massive cyber-attacks disrupt the operation of the Odesa Sea Port, including transportation and cargo handling. The branches of Oshchadbank and PrivatBank banking systems in the Odesa region were attacked.

In a month after the first cyber-attack on Liebherr's internal network in Germany, there have been a series of minor cyber-attacks on the Liebherr's port cranes all over Europe.

In the maritime domain, Bastan's Navy ships are increasing their presence in the Senta's EEZ, using navy exercises and interrupting the international passenger and cargo sea transhipment.

Inject 3.5.1: Day 53: February 27, 11:00

In the last five days, two explosions sank two cargo vessels owned by Senta and Zestan, proceeding to Sea Port Pivdennyi. Two buoyant WWII contact mines are detected by surveillance planes and eliminated by the Senta Navy. The government of Zestan releases initial technical evidence compromising the assumption about old contact mines: all damage is located deeper under the hull, near the stern, and all explosions hit the engine room. Some international shipping companies declare Senta's EEZ as dangerous for shipping.

Response to Inject 3.5.1

Contrary to previous injects, now the Ministry of Foreign Affairs does not need to consider those other ministries. We can now easily confirm to international community that two explosions have occurred, these disrupt the supply chain and it must be known to the international community. This seems clear enough that a message needs to be delivered to the international community to receive a response. It is not only press releases that must occur, all of our embassies need to be notified immediately and all diplomatic channels must be used to immediately understand the importance and urgency of this matter and that it is out of control. The mechanism of the UN should be utilized as part of UNCLOS regarding the areas that have been mined.

Recommendation: Ensure Senta processes to gather crucial allied ambassadors in Kyiv for briefings in an emergency is clear. Consider how to have a process to bring together allied ambassadors with Senta officials for a public call for investigation or action.

Inject 3.5.2: Day 54: February 28, 08:00

Major explosions at Ammonia production and storage facilities in PJSC 'Odesa Portside Plant'. Significant release of ammonia and other hazardous chemicals in the atmosphere as a result of an explosion. Dozens of casualties are reported in the plant. The toxic cloud of ammonia is heading towards Odesa city and neighbouring towns. Bastan media and some of Senta media report that the incident was staged as a provocation by Senta's security services.

Response to Inject 3.5.2

International organizations will be immediately made aware of the situation. A joint working group on emergency response should be used to establish a joint response to the hazardous release of chemicals. NATO should be involved. We have bilateral agreement with our partner states regarding emergencies that needs to be utilized. Military from partner nations with hazardous spill specialists may be able to assist - look to European Union's capabilities.

Recommendation: Need to modify and create better Joint working group with EU partners for emergency responses.

Inject 3.5.3: Day 54: February 28, 09:00

Bastan's Navy declares a shooting and exercise area dangerous and blocks a sea route to Odesa Sea Port. An intense LIVEX, including the use of various arms systems, has been ongoing for two weeks and is situated in the vicinity involving merchant vessels navigating through the area - disrupting shipping activities.

Response to Inject 3.5.3

MFA must increase their cooperation with NATO. The current process works, but it takes time. We need to speed it up, so state bodies can feed info to NATO on their own. In addition to set procedures, it is necessary to use the crisis center as a quick response center. Emergency documents can be sent directly to the Office of the President. Once a state of emergency is declared, responses happen quicker. The economic impact of continual LIVEX by Bastan's Navy, of which disrupts shipping, must be apparent to the international community, and requests for assistance can be based on this economic impact need.

Recommendation: NATO needs a very specific list of requested assistance to be able to respond quickly and provide the assistance. Simply asking for help is not enough, the specifics of what is needed must be voiced clearly to NATO. A template for supplying info to NATO for assistance for different scenarios should be developed, to ensure quick response capability. Use April 2021 model, when Ukraine made an effective appeal to NATO as Russian troops massed in east.

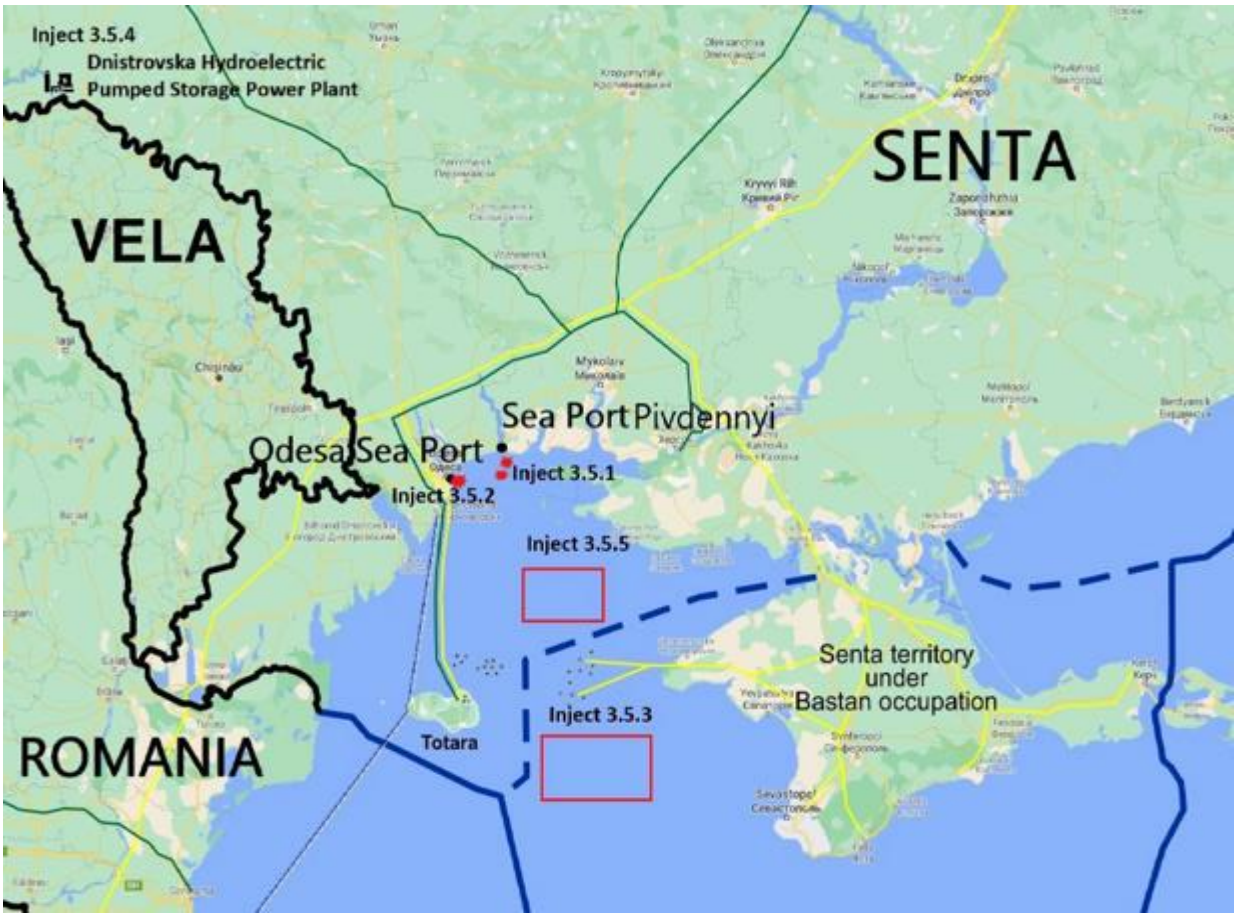
Recommendation: Utilize a collective appeal of all Noir Sea nations to UN to demand Bastan move the coordinates of their exercise out of the shipping lanes due to the economic disruption. The goal is to draw attention to the issue internationally, even if nothing changes.

Inject 3.5.4: Day 55: March 1, 00:00

A cyber-attack is suspected at Dnistrovska hydroelectric pumped storage power plant. After an update of several Programme Logic Controllers (PLC), communication of industrial operations is unstable. Unrealistic readings are provided to the operator on power generation values. Moreover, suddenly all gates rise to maximum height, causing an uncontrolled and unscheduled outflow of water. This sudden outflow damages the turbines at the hydroelectric power plant, as well as causing rapid and massive flooding downriver.

Inject 3.5.5: Day 55: March 1, 11:00

South Senta Nuclear Power Plant is suddenly forced into an emergency shutdown.
Bastan media blame the US nuclear fuel supplier and Senta's 'corrupted authorities' reports that a significant incident occurred in the nuclear power plant with an essential release of radiation.



Inject 3.5.6: Day 55: March 1, 12:00

Bastan establishes a control zone where ships bound to Senta are stopped and searched by Bastan's Navy, the coast guard, or both. Motivation for these acts, as announced by Bastan, is a suspected terrorist threat against undefined strategic targets. Ships are subjected to random controls. Delays are ranging from five hours to two days. The average waiting time per vessel is 20 hours.

Response to Inject 3.5.4/5/6

The Hydro power plant will involve the Ministry of Energy and the State Emergency Service of Senta. The river supplies Senta and also Vela. There are a lot of Noir Sea coastal agreements, but proactive and practical steps must be taken to communicate and enact these. Escalation must occur as quickly as possible to ensure consulates are involved, which is difficult to enact.

Recommendation: Outdated bilateral agreements between Senta and Romania exist for protection and must be updated. These will be an efficient way to get assistance but they must include actions to ensure how partners are to be involved in assistance is to be accomplished and to what end.

Recommendation: Immediate appeal to International Atomic Energy Agency should be made if there is any hint of interference with nuclear infrastructure. That will result in a significant, rapid international response and bring experts into Senta. Make the appeal without hesitation.

Recommendation: Senta should seek to join Estonia's NATO Cooperative Cyber Defence Center of Excellence to better address cyber/hybrid warfare questions.

7.4. Vignette 4: Hybrid Warfare

Tensions between Bastan and Senta have reached the highest level ever. Senta's military intelligence reported an unprecedented number of military build-up in Bastan Navy's bases in the Noir Sea. A significant number of provocative accidents have started to occur on Totara Island. Reports of the loss of GPS and GSM signals on the island. The Internet connection on the island was disrupted.

At the same time, Senta continues to experience a growing number of cyber-attacks against governmental and local institutions, and critical service providers. Bastan's and Senta's media aggressively reports about the inability of Senta's central and local authorities to provide critical services for the population. Moreover, top commanders of Senta's armed forces in Kyiv and Navy officials in Odesa and Totara Island received e-mails from unconfirmed accounts with a direct warning 'not to follow orders of Senta's political authorities, or they and their families will be in danger'.

Social media is full of reports and active discussions about the possible separation of the South part of Senta. The same news is being spread via official web pages of regional councils. The above leads to pressure and tensions inside governmental institutions, law enforcement agencies, and armed forces. In the last 24 hours, street manifestations against the Senta government intensified dramatically, namely in the central cities of southern regions: Odesa, Mykolaiv and Kherson. As a result, the government is overstretched, and the population is confused.

Against the background of significant cyber disruptions, psychological pressure, the spread of misinformation, and growing street manifestations in southern regions, suddenly a considerable number of military forces without insignia launched on the Totara Island. The access to the Port of Totara Island is blocked by the cargo ships with no State flag identification. The access by water to the Totara Island is cut off.

The drilling rigs for hydrocarbon production of Totara Island located in the Senta's EEZ were occupied and now are under the full control of armed men with no State identification.

Inject 4.5.1: Day 56: March 2, 05:00

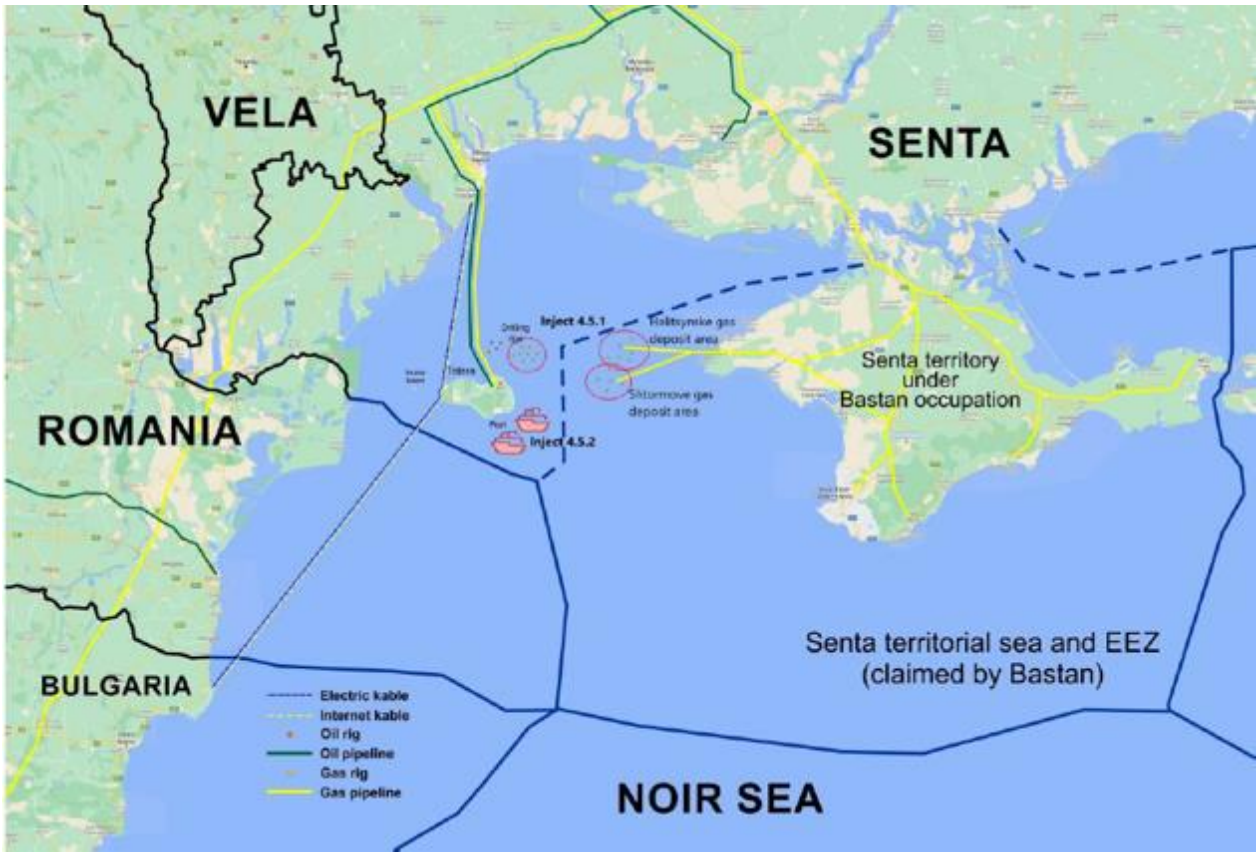
Armed men occupy eight gas rigs off Totara Island in the EEZ of Senta without insignia who used helicopters to land on the rigs and took them over. The Bastan Navy established a control zone around rigs, namely in Shtormov and Halitsyno gas deposit areas. Civilian ships and aeroplanes report significant disruptions of GPS signals in the Noir Sea region.

Response to Inject 4.5.1

Senta military presence must be installed on the island and measures escalated for border patrol forces. Senta should send military immediately to the island due to security issue. Presence of surveillance, patrol, and research ships can be established to let Romania know why Senta is sending troops there.

Inject 4.5.2: Day 58: March 4, 02:00

One month since establishing the control zone in Senta's EEZ, the controlling of SLOCs by Bastan continues. A significant number of heavily armed men without insignia and pro-Bastan activists land on Totara Island at night by helicopters and from civilian cargo ships. Reports about the takeover of local institutions and major Senta's naval base on the island. Cargo ships with no State flag identification are used to block access to the naval base completely.



Response to Inject 4.5.2

Senta does not have an effective tool against Bastan's aggression in the UN Security Council. Senta needs to ensure that the international community is hearing the reality of the situation, instead of the distorted information supplied by Bastan. High level negotiations are required. The unknown armed men and ships must be identified in order to implement sanctions.

Recommendation: It is critical for Senta to continue to ensure the international community is aware of the truth of what is happening. Continual information flow must occur via all possible avenues to make the situation aware to all around the world.

Recommendation: Sanctions principles should be established with regional, European, and NATO member states to ensure imposition of tough and effective sanctions quickly in cases like this, where territorial integrity is breached. Sanctions have proven fairly effective in the past but agreement on details of what to do often comes too slow.

7.5. Vignette 5: Post-Crisis Stabilisation

The present vignette focuses on the post-crisis and recovery stabilisation process. The post-crisis stabilisation takes place after the end of the crisis scenario – from March 7, 20YY. Crisis management issues are to be discussed, as well.

Each syndicate will be presented with several questions for the post-crisis stabilisation discussion.

1. How effective was the response of international organisations and the international community to Bastan's manipulating of international law rules in the context of the capture / cyber-attack of critical infrastructure, the exclusive maritime economic zone, maritime trade routes and Senta's territory?
2. Do international organisations have sufficient leverage in such situations?
3. Should international sanctions against Bastan only apply to its organisations (institutions), individuals directly involved in a crisis, and not to apply to the whole country? What can be the mechanisms for the international community to impose and control such sanctions?
4. What measures should be applied to a country that disregards international law?

Response to Questions

Introducing sanctions for the companies involved in the annexation of the Senta peninsula was highly effective for international organizations in the past, but took Senta a very long time to enact. It is important to collect official information that can fully support legal action against these companies as there is a lack of current Senta legislation to direct this issue. The Security Council is moving in this direction.

Regarding introducing sanctions on Bastan, there are several options dependent on whether they are Senta's or international. The effectiveness of these sanctions varies. A negative is that the UN either does not impose sanctions that have been passed or they are proposed by them but they are constantly blocked. Senta needs to determine who it can get support from regarding imposing further sanctions. For example, the US & EU can support their own ban against buying military equipment from Bastan, it is the 3rd biggest source of income for them.

An effective embargo can be imposed on the export of energy products of the oligarchs as well as seizing the assets of Bastan oligarchs. Sanctions against the actors that are extracting gas from Noir Sea Jack rigs should not allow selling internationally. Senta consumes 80% of fuel from Bastan. There is only one oil refinery factory in Senta with low level utilization due to imports from Bastan. Senta needs to change its policy regarding oil imports to facilitate an increase of local utilization. it is a big challenge on how to make sanctions effective.

When civil unrest begins the Commander-in-Chief gives the order for vessels to start moving into the problem area. Can we ask for help from Romania? Can we make a request from our partner states for humanitarian assistance in the form of diesel fuel for our ships and humanitarian relief of fuel supplies? This is not an easy issue to solve with unanswered questions.

We should keep in mind that in the case that Odesa is occupied by separatists, what will we do next? Besides sanctions, we have some NATO mechanisms we can use. Who else can we rely on for assistance? What are the expectations of them? There are some areas that are beyond STRATCOM, influential people

who are leaders of opinion. Does MOFA have a list and constant cooperation? Working with opposition leaders of Bastan to increase help.

Noir Sea working group meets from various countries in the Noir Sea, they share their experiences. There are groups of lawyers also who support these causes. How do they communicate with the population? Our learning centers must be used to highlight the circumstances that took place and all the legal ramifications of what was done and what laws were broken. Ensuring it is known to society.

There is NATO Parliamentary Assembly and an interparliamentary council. Effective work with international community must occur from day 1. This must occur at the very first stages, before seizing of vessels, etc.

Recommendation: in case of hybrid war, Senta should be comfortable with making multilateral international requests for assistance, but not be stuck waiting for slow-working bodies to come to decisions. Senta must be able to ask for and receive assistance multilaterally with a rapid turn-around and no hesitation.

7.6. Key Takeaways

* Readers should note that this syndicate embedded several recommendations within its responses to specific vignette/injects that are not included in Key Takeaways.

International Partner Response There is a need for tailor made solutions to counter threats related to political, legal, economic, and energy issues. National and international legal acts are required regarding protection of critical infrastructure and energy security issues at high level. Immediate actions are also needed to facilitate the appropriate presidential and governmental response in coordination with international partners to counter conflict situations. **Recommendation**: The revival and modification of a NATO-Ukraine Joint Working Group on Economic Security is recommended. The updating of the legislation of Ukraine is required and should be implemented under the Association Agreement between Ukraine and the EU. This will strengthen the country's energy independence during a crisis by ensuring a minimum stock of oil and oil products; the creation of gas insurance reserves (according to EU recommendations), and the improvement of a legal framework to strengthen trans-border relations and cooperation. Support increasing local hydrocarbon, gas, and oil production alongside refinery and petrochemical development. Adopt EU regulation in Ukraine for infrastructure projects as well as the deployment of infrastructure for alternative and decarbonized fuels. Involve members of the Ukrainian parliament to initiate requests to the parliaments of other states, and also use the options of NATO Parliamentary Assembly.

International Agreements Enforcement by the parties of the obligations of legal agreements and any possible amendments is required. Updating international treaties will create a basis for utilizing the international court system in the event of conflict. **Recommendation:** Revise the already existing multi-national agreements (i.e. Budapest Memorandum, United Nations Convention on the Law of the Sea, Statute of Black Sea Economic Cooperation). Evaluate all international agreements regarding Ukrainian border cooperation; specifically, emergency, environmental, and military interactions in times of crisis. Improve technical capacities for intelligence information exchange utilizing the Enhanced Opportunity Partnership. Involve civil society and subject matter experts to increase international awareness and promote Ukrainian positions enhancing systematic interaction with opinion-makers and decision-makers

in partnering states. Create a national evidence-based database of international treaty violations focused on high conflict areas.

Internal Preparedness for International Cooperation Adaption of some of the most relevant national instruments to the challenges related to energy security issues in order to facilitate the process of forming legally binding ground for a consolidated international response is required. This will avoid violation of national law creating a favorable and productive environment for the development of international relations. **Recommendation**: The development of interregional cooperation by Ukraine is extremely important at the beginning of conflict in order to avoid creating an environment for escalation. Create a branch network of situational awareness centers to improve cooperation between Ukrainian state bodies in the event of crisis. Develop a National Action Plan on Maritime Security and establish a Ministry of Foreign Affairs (MFA) and Foreign Intelligence Service of Ukraine cooperation for immediate information exchange and better preparedness. Establish an information request mechanism between the Ukrainian state agencies and the MFA regarding their needs from international organizations to avoid overlapping of efforts and to provide appropriate coordination. Develop an appropriate coordinated action to predict and resist energy threats towards Ukraine, the European Union, and other countries in the region. Implement international exercises between units of the armed forces of Ukraine, the National Guard of Ukraine, the National Police of Ukraine, and the State Border Guard Service of Ukraine with corresponding units of foreign countries.

8. Conclusion

CORE 20 was a national-level exercise aimed at enhancing resilience of Ukraine's critical infrastructure systems through high-level interagency participation. The engagement served as a critical platform for collaborating with over 150 participants from 15 countries and more than 50 organizations. The sequence of presentations and syndicate work was both informative and instrumental in identifying critical infrastructure resiliency gaps, mitigation strategies, best practices, and recommendations applicable to the Government of Ukraine.

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 are captured below.

During the Distinguished Visitor Day, Olha Stefanishyna, the Deputy Prime Minister for European and Euro-Atlantic Integration*, provided keynote remarks regarding the importance of the NATO CORE20 TTX in furthering Ukraine's resilience.*

8.1. Concluding Exercise Key Takeaways and Recommendations

Areas for Improvement

Economic resilience requires greater focus. Currently, the emphasis for resilience is on physical security of infrastructure and protecting energy systems. What remains is other risk such as supply shortfalls due, political risk, to energy supplies. It is necessary to have sufficient and continuous energy supplies to enable

the systems to function. Greater energy diversity and storage is required to protect against supply disruptions. Resilience alone does not ensure supply. **Recommendation:** Fuel and other critical supplies (food. Water, critical materials) require adequate storage levels based on supply chain cycles and operations.

Shortfalls in Technically Qualified Personnel. Too often, educated and experienced personnel move abroad leaving critical shortfalls in necessary technical skills and experience to maintain resilience. The standard notice to end employment is four weeks. This is not enough time to replace such qualified personnel. **Recommendation:** Consider long term contracts for technically qualified personnel responsible for critical infrastructure and consider other measures to limit such "brain drain." through government, industry, and academic partnerships that lead to jobs and benefits.

Below Ministry Interagency Cooperation. Each governmental agency, below ministerial, is aware of its own roles and responsibilities and have corresponding capabilities, and each operates on its own based on ministry guidance and not in concert with other agencies within its ministry or beyond. Participants recognized the requirement for greater interagency cooperation to best ensure resilience of critical infrastructure and energy systems. There is no formal regulatory mechanism to identify the processes of how such interaction should take place. **Recommendation:** Formal interagency mechanisms need to be developed to formalize interagency cooperation. Once developed, departmental personnel also require training on the practical aspects of conducting such communications and liaisons. Such interactions should be exercised at each level, across agencies and regions, and critical infrastructure sites, example a port.

During the Distinguished Visitor Day, COL Darius UŽKURAITIS, the Director of the NATO Energy Security Centre of Excellence provides an overview of the NATO CORE 20 TTX in Odesa, Ukraine.

Designation of Critical Infrastructure. No universal government definition of 'critical infrastructure' has been agreed upon by all Ukrainian agencies. As a stopgap measure the internal security services (SBU) have generated an independent list of critical infrastructure assets that has not been shared with the other agencies. As no legislated definition of the term exists, no subsequent staffing, coordination, and

evaluations occur. **Recommendation**: Identify a lead agency to support the passage of required laws and legislation which will enable the building of resilient systems. The National Parliamentary Committee is still in process regarding this resolution. Currently there is a resolution in front of the Cabinet of Ministers to define critical infrastructure facilities. Ministries have few experts to focus on the issues and might need outside support in the process.

Requirement for Closing Perspective Seams Amongst National Resilience Entities. As a result of concurrent and consecutive non-traditional methods Bastan and unidentified armed men employed to create conflict and crisis situations, the transition of decision making at the national, regional and local levels was inconsistent, and the applicable legal framework and regulation for national and regional coordination amongst agencies/bodies was not transparent. **Recommendation**: Improve readiness of national resilience entities by implementing a framework for the early-inclusion and wide interaction of all entities regarding hybrid threats, so the transition of responsibility amongst entities is less subject to continuity gaps/problems.

Resolve/Remove the Uncertainty of the Organizational Model of Ensuring National Resilience. A unified/single methodology for assessing risks to national security and state of relevant capabilities to prepare, make and implement decisions was frequently debated amongst the Armed Forces, National Security and Defense Council and Anti-Terrorism Center of Senta. **Recommendation**: Ensure the implementation of a strategic document in the field of maritime security, which, in particular, defines the basis for the protection of national interests at sea and implementation of a risks management system, in particular, their assessment and development of measures to minimize their impact.

During the Distinguished Visitor Day, participants and facilitators listen to syndicate out briefs.

Best Practices/Strengths

Crisis Communications. The State Service of Special Communications of Ukraine is an independent agency/service that effectively provides crisis communications for all agencies, regions, and sites and is further responsible for aspects of strategic communications. Embedded, is a National Telecommunications and Special Communications Centre that provides emergency communications lines among all agencies and ensures functional command and control of the government. The communications system cannot be hacked, interfered with, damaged, or turned off. **Recommendation:** This effective state controlled and funded national communications apparatus should be considered for partner nations that may lack such a robust system.

Understanding and Mitigation of Russian Misinformation Campaigns. Russian disinformation has been effective at spreading misinformation, creating divisions, and degrading trust in targeted regime's ability to govern. However, in the past several years, Ukraine has many lessons learned to mitigate and counter Russian disinformation such as its successes building population trust, disproving fake propaganda and today a large portion of Ukraine population can discern between fake and real information. Russia now lacks the ability to change Ukraine minds, however; there are some Pro-Russian Ukrainians who will support Russian disinformation regardless. **Recommendation:** Ukraine's capabilities to counter Russian disinformation campaigns are beneficial to other nations confronting similar threats.

Strengthened Resolve Among Population. Ukraine has recognized that during times of crisis when security forces are stretched in response to major incidents and operations, the population does not seek to take advantage through looting and criminal activity. In this senses, Russia's attempt to weaken Ukraine strengthened many Ukrainian resolve to makes sacrifices in order to maintain Ukraine's sovereignty and reject Russia's malign activities.

During the Distinguished Visitor Day, the Representative of the Government Office, Col. Serhii VERBYTSKYI, *presents welcoming remarks in Odesa, Ukraine.*

8.2. Closing

It is important to note that this report – ideally – does not end CORE 20, for Ukraine 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 analyze the key takeaways pertinent to their organizations to identify the best means to facilitate improvements and develop the corresponding plan of action to make such positive changes in order to improve the 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 (six months, one year, etc.) to survey participants on any improvements that were implemented based on what was learned from CORE 20. After CORE20 TTX Presidential Decree regarding National Resilience Concept was signed on 27 Sep 2021, Critical Infrastructure Law enacted on 16 Nov 2021 and the Maritime Security Strategy of Ukraine was approved on 11 February 2022 by the Security and Defence Council of Ukraine.

CORE 20 FAMILY PHOTOGRAPH.

Addendums

List of Participating Organizations

- NATO HQ
- NATO Allied Command Transformation
- NATO Energy Security Centre of Excellence
- NATO Maritime Security Centre of Excellence
- NATO Strategic Communications Centre of Excellence
- NATO Collective Cyber Defense Centre of Excellence
- NATO Special Operations Headquarters
- NATO Representation to Ukraine
- Hybrid Centre of Excellence
- US Naval Postgraduate School
- National Institute for Strategic Studies of Ukraine
- National Defence University of Ukraine
- NATO Information and Documentation Center
- Embassy of Canada
- Embassy of the Kingdom of Belgium to Ukraine
- Embassy of the Republic of Bulgaria to Ukraine
- Embassy of the Kingdom of Denmark to Ukraine
- Embassy of the Republic of Estonia to Ukraine
- Embassy of the Republic of Finland to Ukraine
- Embassy of Georgia to Ukraine
- Embassy of the Federal Republic of Germany to Ukraine
- Embassy of Japan to Ukraine
- Embassy of the Republic of Lithuania to Ukraine
- Embassy of the Republic of Moldova to Ukraine
- Embassy of the Kingdom of Norway to Ukraine
- Embassy of Romania to Ukraine
- Embassy of the Republic of Slovakia to Ukraine
- Embassy of the Kingdom of Sweden to Ukraine
- Embassy of the Turkish Republic to Ukraine
- Embassy of the United Kingdom to Ukraine
- Embassy of the United States of America to Ukraine
- National Security and Defense Council of Ukraine
- Security Service of Ukraine
- Ministry of Internal Affairs of Ukraine
- Ministry of Defense of Ukraine
- Ministry of Economy of Ukraine
- Ministry of Infrastructure of Ukraine
- Ministry of Foreign Affairs of Ukraine
- Ministry of Justice of Ukraine
- Ukrainian Armed Forces

- Ukraine Navy
- State Service for Special Communication and Information Protection of Ukraine
- State Emergency Service of Ukraine
- Ukraine National Police
- Ukraine National Guard
- Odesa State Regional Administration
- NAFTOGAZ
- UKRENERGO
- Gas Transmission Operator of Ukraine
- Ukrainian Railway (Odesa Branch)
- Office of the President of Ukraine
- Ukraine National Coordination Center for Cyber Security
- Ministry of Culture and Information Policy of Ukraine
- State Border Guard Service of Ukraine
- State Committee For TV & Radio Broadcasting of Ukraine
- Ukraine Mission to NATO
- NGO “Ukraine Prism”
- Sea Port Administration of Ukraine
- National Bank of Ukraine
- Government Office for Coordination of European and Euro-Atlantic Integration

Results of Participant Exercise Evaluation Surveys

Evaluation of CORE 20 Tabletop Exercise – Comments Analysis from Participant Exercise Evaluation Surveys

Evaluation by participants (Annex 3) during the course of the TTX shows that the majority of the participants marked this type of event as highly beneficial – a large majority expressing that the aspect "most liked" about the exercise was the chance to engage and dialogue with other agencies and foreign partners. Many participants also cited that they liked the scenarios chosen for the exercises, specifically because of their realism and applicability to real-life scenarios. Several comments spoke to the high level of organization of the tabletop exercises, discussions, and presentations.

When asked to describe what participants least liked about CORE TTX, a large number of participants commented on how they disliked not being able to interact with other syndicates during discussions. Several participants commented on how there was little time to discuss the scenarios, vignettes and injects. One possible reason for the short amount of time for discussion(s) was cited as being due to the length of time it took for translations. Another source, as referenced by some participants, could be the "constant change of the format of presentations."

When asked for suggestions on ways CORE TTX could be improved, a large number of participants suggested structural changes to the syndicates. Suggestions included to: 1) "make another syndicate which would encompass all other syndicates, [with the overall objective to] to make a final assessment; 2) decrease the number of syndicates, so as to make more efficient, concise groups involving both military and civilian representatives; 3) conduct tabletop exercises on a regular basis and invite more experts from other agencies, such as ministry of health and ministry of infrastructure and 4) all for the syndicates to interact and dialogue with one another during exercises.

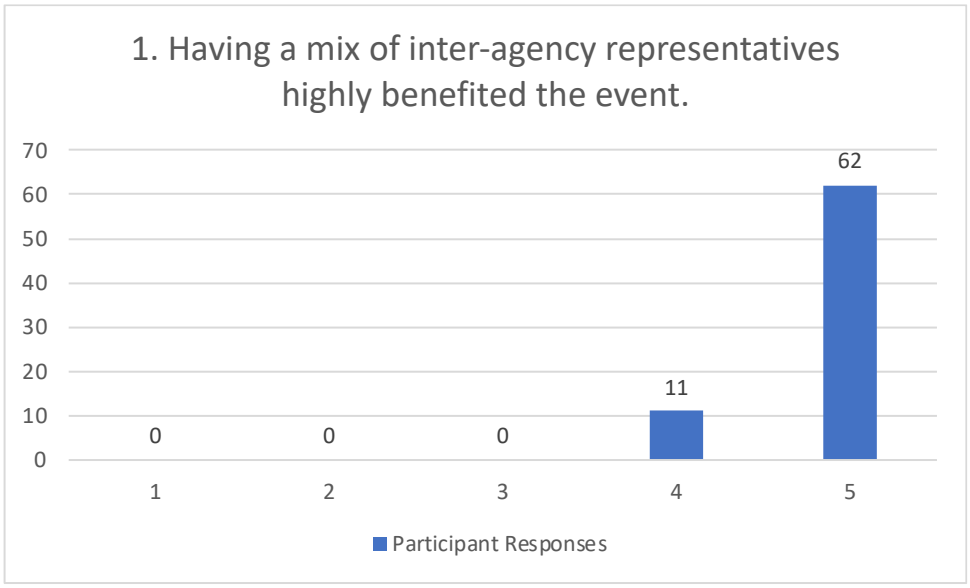
Similarly, many suggestions called for honing the practicality and applicability of the scenarios. For example, a few suggestions were made to have more "practical" tasks focused on cyber security, technical cases, and examples related to organizational work.

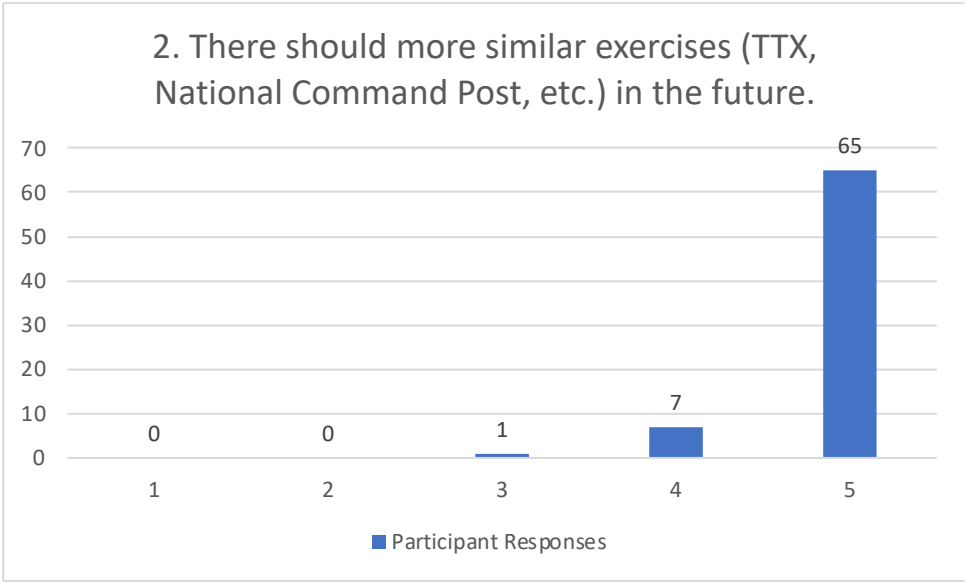
Many participants also suggested to allow for more time for discussion and analysis of vignettes, and to allow team leaders 20-30 minutes to finalize the course of action regarding vignettes. Suggestions were also made to "better inform" participants on the goals and tasks expected of them during the exercises before they begin.

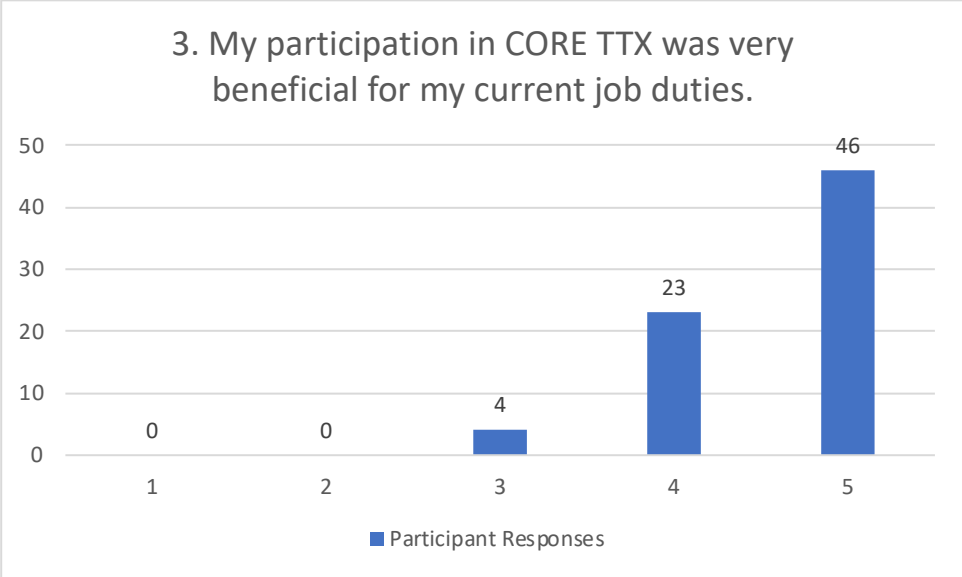
Results of Participant Exercise Evaluation Surveys

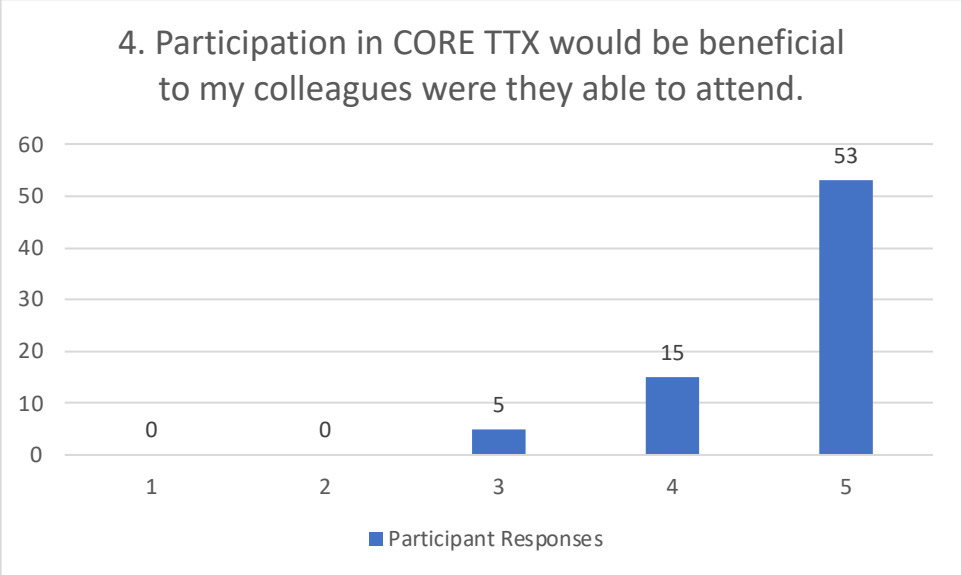
Quantitative Response Part I

- **Please answer the following questions/statements on a scale of 1 to 5 with 1 being STRONGLY DISAGREE and 5 being STRONGLY AGREE:**





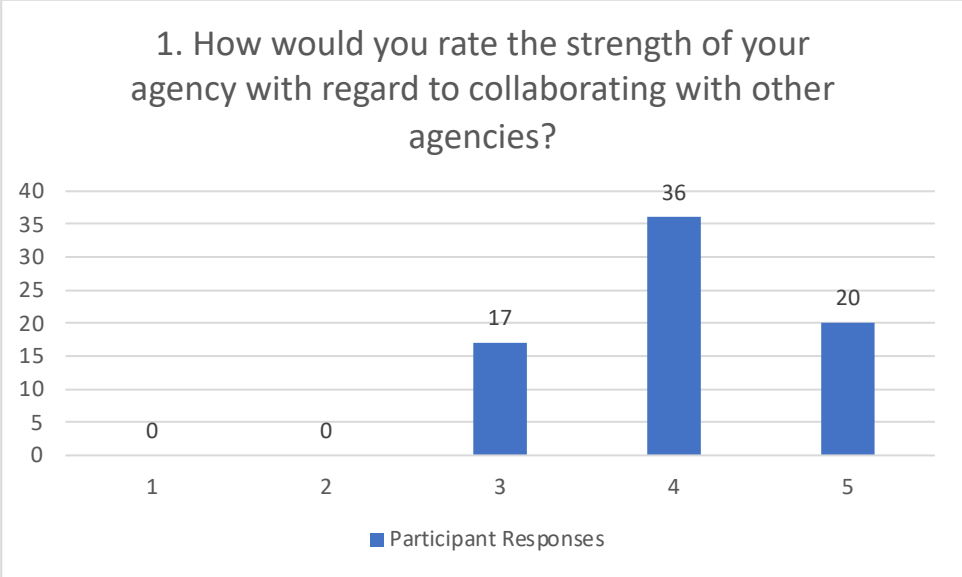

3. My participation in CORE TTX was very beneficial for my current job duties.
50
40
30
20
10
0
0
0
4
23
46
1
2
3
4
5
Participant Responses

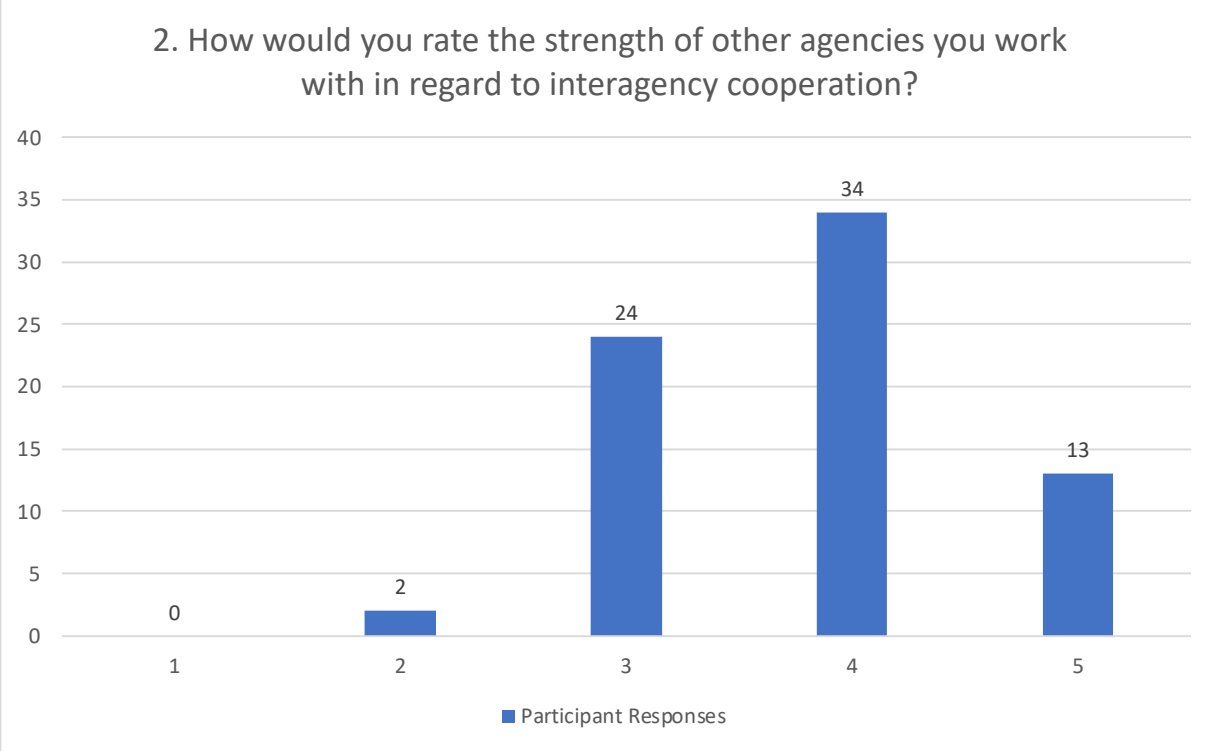

4. Participation in CORE TTX would be beneficial to my colleagues were they able to attend.
60
50
40
30
20
10
0
0
0
5
15
53
1
2
3
4
5
Participant Responses

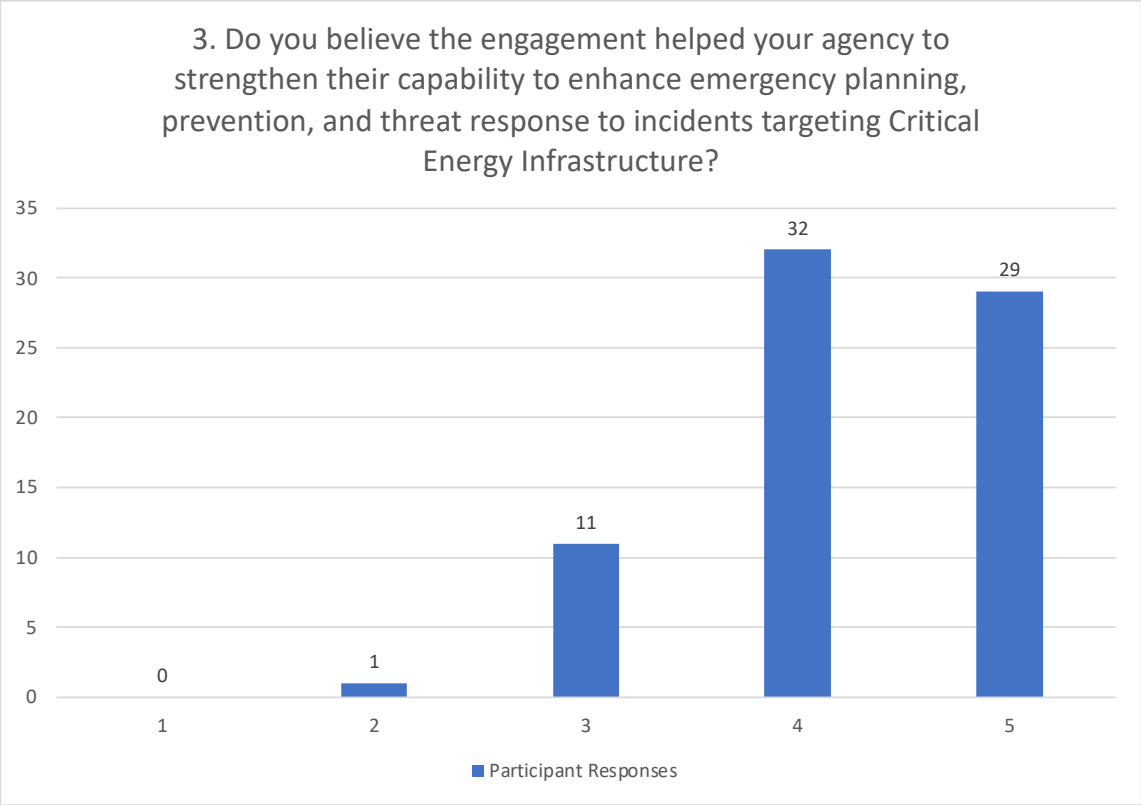
Quantitative Response Part 2

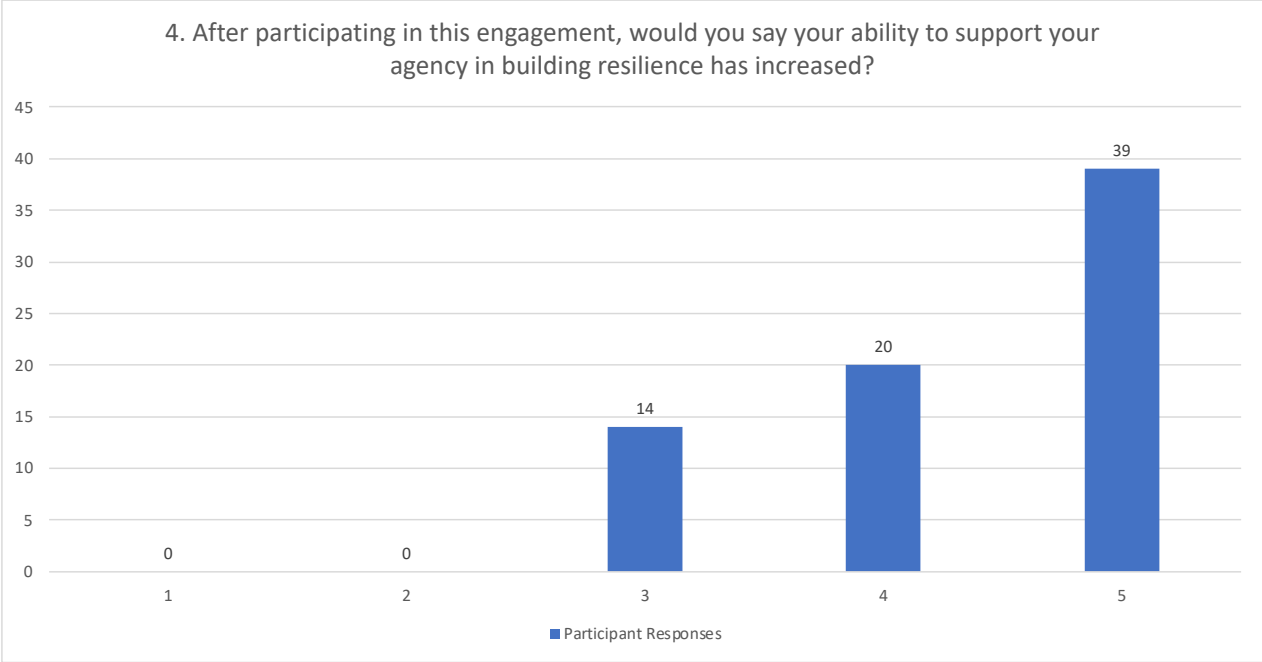
- **Please answer the following questions on a scale of 1 to 5 with**

1 being NEEDS MUCH IMPROVEMENT/STRONGLY DISAGREE and 5 being VERY STRONG/STRONGLY AGREE:






3. Do you believe the engagement helped your agency to strengthen their capability to enhance emergency planning, prevention, and threat response to incidents targeting Critical Energy Infrastructure?
35
30
25
20
15
10
5
0
0
1
11
32
29
1
2
3
4
5
Participant Responses


4. After participating in this engagement, would you say your ability to support your agency in building resilience has increased?
45
40
35
30
25
20
15
10
5
0
0
0
14
20
39
1
2
3
4
5
Participant Responses

Glossary of Acronyms

Acronym	Definition
AAR	After Action Review
CEI	Critical Energy Infrastructure
ICS	Industrial Control Systems
IP	Improvement Plan
IS	Independent Study
IT	Information Technology
NPP	Nuclear Power Plant
kV	Kilovolt(s).
GW	Gigawatt
SCADA	Supervisory Control and Data Acquisition
TTX	Tabletop Exercise
UES	United Energy System

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, to meet an intended
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;
Critical Infrastructure	Enterprises and institutions (regardless of ownership) of such industries as energy, chemical industry, transport, banks and finance, information technologies and telecommunications (electronic communications), food, health care, utilities, which are strategically important for the functioning of the economy and security of the state, society and population.
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
Sabotage	Commitment in order to weaken the state of explosions, arson or other acts aimed at mass destruction of people, causing bodily harm or other damage to their health, destruction or damage to objects of significant economic or defense significance, as well as committing with that the very purpose of the action aimed at radioactive contamination, mass poisoning, the spread of

Term	Definition
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"
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
Maritime Security	An international and interagency, civil and military, activity to mitigate the risk and counter the threat of illegal or threatening activities in the maritime domain, so that they may be acted upon in order to enforce law, protect citizens and safeguard national and international interest. Maritime Security will therefore concentrate on the unlawful use of the maritime domain.
Maritime Security Operations	The action carried out at sea by those military and civil authorities equipped with the appropriate assets and empowered to act upon Maritime Security related risks and threats.

Term	Definition
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
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

Term	Definition
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
United Energy System (UES of Kray)	A set of power plants, electric networks, other objects of electric power, combined by a common mode of production, transmission and distribution of electric energy with centralized management of this regime

Here the "Golden Child" monument is displayed at the Odesa port outside the CORE 20 TTX venue.