



Непорушна стійкість 2020 CORE20 Командно-штабні навчання Кінцевий звіт про навчання

13-17 вересня 2021 року
Одеса, Україна

21 квітня 2022 року

Академічна група з енергетики Школи післядипломної освіти ВМС США (NPS EAG), Центр передового досвіду НАТО в галузі енергетичної безпеки (ENSEC COE)

Зміст

1. Вступ	5
1.1. Програма «Непорушна стійкість»	5
1.2. «Непорушна стійкість 20» (CORE 20) - Україна	5
1.2.1. Огляд	5
1.2.2. Мета, ціль, основні завдання	5
1.2.3. Концепція Заходу	6
1.2.4. Кінцевий звіт про навчання	8
2. Сценарій Командно-штабних навчань CORE 20	10
2.1. Передумови і Сценарій	10
2.2. Геополітична ситуація	10
2.3. Соціально-економічна ситуація	11
2.4. Метеорологічна обстановка та ситуація з попитом на газ	12
2.5. Безпека критичної інфраструктури в регіоні	12
2.6. Ситуація з морською безпекою	14
2.7. Кібербезпека і радіоелектронна боротьба	15
2.8. Комунікація та повідомлення засобів масової інформації	16
2.9. Висновки щодо сценарію	17
2.10. Розділ про епізоди та ввідні	17
2.11. Структура епізодів та ввідних	17
3. Синдикат (Група) 1: ЗКІ від небезпек, загроз і атак	22
3.1. Епізод 1: Доконфліктна фаза: Гібридний вплив	22
3.2. Епізод 2: Гібридні операції низької інтенсивності	25
3.3. Епізод 3: Фаза конфлікту: Гібридні операції високої інтенсивності	30
3.4. Епізод 4: Гібридна війна	34
3.5. Епізод 5: Посткризова стабілізація	36
3.6. Ключові висновки	37
4. Синдикат (Група) 2: Кібербезпека	39
4.1. Епізод 1: Доконфліктна фаза: Гібридний вплив	39
4.2. Епізод 2: Гібридні операції низької інтенсивності	43
4.3. Епізод 3: Фаза конфлікту: Гібридні операції високої інтенсивності	48
4.4. Епізод 4: Гібридна війна	54

4.5.	Епізод 5: Посткризова стабілізація	57
4.6.	Ключові висновки	58
5.	<i>Синдикат 3: Морська безпека</i>	61
5.1.	Епізод 1: Доконфліктна фаза: Гібридний вплив	61
5.2.	Епізод 2: Гібридні операції низької інтенсивності	65
5.3.	Епізод 3: Фаза конфлікту: Гібридні операції високої інтенсивності	68
5.4.	Епізод 4: Гібридна війна	71
5.5.	Епізод 5: Посткризова стабілізація	73
5.6.	Ключові висновки	75
6.	<i>Синдикат 4: СТРАТКОМ.....</i>	77
6.1.	Епізод 1: Доконфліктна фаза: Гібридний вплив	77
6.2.	Епізод 2: Гібридні операції низької інтенсивності	80
6.3.	Епізод 3: Фаза конфлікту: Гібридні операції високої інтенсивності	84
6.4.	Епізод 4: Гібридна війна	88
6.5.	Епізод 5: Посткризова стабілізація	90
6.6.	Ключові висновки	91
7.	<i>Синдикат 5: Міжнародне реагування/Міжнародне право</i>	94
7.1.	Епізод 1: Доконфліктна фаза: Гібридний вплив	94
7.2.	Епізод 2: Гібридні операції низької інтенсивності	98
7.3.	Епізод 3: Фаза конфлікту: Гібридні операції високої інтенсивності	102
7.4.	Епізод 4: Гібридна війна	106
7.5.	Епізод 5: Посткризова стабілізація	108
7.6.	Ключові висновки	109
8.	<i>Підсумки.....</i>	111
8.1.	Ключові висновки та рекомендації, підбиваючи підсумки проведеного навчання	111
8.2.	Закриття навчань	115
	<i>Додатки</i>	116
	<i>Список організацій-учасниць.....</i>	116
	<i>Результати опитування учасників щодо оцінки навчань.....</i>	118
	<i>Глосарій скорочень</i>	123
	<i>Глосарій термінів.....</i>	124



1. Вступ

1.1. Програма «Непорушна стійкість»

«Непорушна стійкість» (CORE) – це серія командно-штабних навчань (КШН) на національному та регіональному рівнях, розроблена Центром передового досвіду НАТО в галузі енергетичної безпеки (ENSEC COE), які спрямовані на підвищення стійкості енергетичних систем в епоху гібридних загроз. КШН CORE проводяться в Україні з 2014 року, як і програми на національному та регіональному рівнях в країнах Балтії. CORE 20 були другими українськими КШН CORE, а їх розробка була схвалена Платформою Україна-NATO з протидії гібридній війні та в рамках європейської та євроатлантичної інтеграції України.

1.2. «Непорушна стійкість 20» (CORE 20) - Україна

1.2.1. Огляд

Визнаючи стратегічну важливість Чорноморського регіону для НАТО і його партнерів, міністри закордонних справ країн-членів НАТО вирішили посилити практичну підтримку України, що стосується Чорного моря, в тому числі співпраця з Військово-морськими силами України, ситуативна обізнаність, відвідування портів, навчання й обмін інформацією. КШН CORE 20 були заплановані як частина цієї підтримки з метою підвищення стійкості України до гібридних ризиків і її спроможностей реагувати на кризові ситуації шляхом покращення міжвідомчої та військово-цивільної координації, планування й готовності. Після кількох перенесень через COVID-19 захід було проведено 13-17 вересня 2021 року.

1.2.2. Мета, ціль, основні завдання

Командно-штабні навчання CORE20 були розроблені за підтримки Відділу політичних питань і політики безпеки Штаб-квартири НАТО (PASP), Відділу нових викликів безпеки Штаб-квартири НАТО (ESC), Центру передового досвіду НАТО в галузі енергетичної безпеки (NATO ENSEC COE) і Кабінету Міністрів України, аби сприяти владі України у питанні підвищення стійкості шляхом поліпшення готовності до надзвичайних ситуацій, планування, запобігання і реагування на загрози. Крім того, CORE20 були націлені на зміцнення потенціалу України щодо захисту критично важливої інфраструктури, морського та кіберпростору, а також енергетичних систем.

Ціллю КШН, зосереджених на Чорноморському регіоні, було розширення спроможностей українських національних і місцевих органів влади щодо реагування на кризові ситуації і підвищення стійкості у світлі гібридних загроз критичній інфраструктурі та енергетичним системам за допомогою ефективної міжвідомчої координації, військово-цивільної координації, планування, готовності та співпраці між державним і приватним секторами.

Для CORE20 були визначені такі основні завдання:

- Оцінка стійкості критичної інфраструктури України та готовності протистояти гібридним загрозам (дезінформація, кібератаки, диверсія, таємні операції);
- Перевірка ефективності національних планів, регламентів і процедур антикризового управління щодо реагування та зниження наслідків і можливого впливу гібридних дій (зокрема, у сфері енергопостачання);
- Відпрацювання планів з підвищення безпеки критичної інфраструктури і ланцюгів постачання, зокрема, Генерального штабу;
- Оцінка процедур стратегічних комунікацій для зниження впливу ворожої дезінформації, в тому числі стратегії, плани та механізми комунікації в кризових ситуаціях;
- Оцінка здатності координувати дії з країнами-членами НАТО, державами-партнерами та міжнародними організаціями

1.2.3. Концепція Заходу

На відкритті CORE 20 з вітальним словом виступили директор Центру передового досвіду НАТО в галузі енергетичної безпеки, полковник Даріус УЖКУРАЙТИС (Darius UŽKURAITIS) і керівник відділу співробітництва з НАТО (у сфері оборони та безпеки) Урядового офісу, полковник Сергій Вербицький.



Під час свого вітального слова, полковник Сергій ВЕРБИЦЬКИЙ в Одесі, Україна.

Тиждень був розділений на три фази, які включали академічний семінар, КШН і день високоповажних гостей/підбивання підсумків.

Перша фаза – академічний семінар – включала серію презентацій експертів, аби краще підготувати учасників до КШН. Лекції 1-го дня включали такі теми: «Гібридні загрози критичній енергетичній інфраструктурі», представлена паном Флоріаном Енке і паном Юліюсом Грубляускасом (обидва зі штаб-квартири НАТО); «Ціль гібридних атак: критична інфраструктура», представлена доктором Олександром Суходолею (Національний інститут стратегічних досліджень, Україна); «Міжнародне право і гібридна війна», представлена доктором Ганною Шелест (керівник безпекових програм, Рада зовнішньої політики «Українська призма»); «Кібербезпека критичної інфраструктури», представлена доктором Олександром Потієм (заступник голови Державної служби спеціального зв'язку та захисту інформації) і паном Валентином Петровим (Рада національної безпеки та оборони України); та «Міжнародне право і гібридна війна», представлена паном Сергієм Карасовим («Lano Solutions»).



Під час семінарської частини програми КШН «CORE 20 – Чорне море» учасники та координатори заслухали виступи експертів з таких тем, як стратегічні комунікації та кібербезпека.

Лекції 2-го дня академічного семінару включали такі теми: «Морські аспекти гібридних загроз», представлена лейтенантом Олександром Гудіштяну (Військово-морський флот Румунії, Центр передового досвіду НАТО в галузі морської безпеки); «Протидія гібридним діям військовими і невійськовими організаціями (Національна безпека та оборона)», представлена капітаном Степаном Яким'яком (Україна, Національний університет оборони України); «Стратегічні комунікації та гібридні загрози», представлена полковником Дугласом Кохраном (1 німецько-нідерландський корпус); «Основні інформаційні операції Кремля в Україні з 2014 року», представлена пані Любов'ю Цибульською (Український кризовий медіацентр); «Кіберстійкість», представлена майором Емре Халісдемір (Республіка Туреччина, Центр передового досвіду спільного кіберзахисту НАТО); та «Практичні моделі міжвідомчої та міжнародної співпраці при протидії гібридним загрозам», представлена паном Олександром Данилюком (Центр оборонних реформ, Київ) і л-нт командером

Озгюром ДЮНДАРОМ (Республіка Туреччина, Центр передового досвіду НАТО в галузі енергетичної безпеки). У кінці 2-го дня, на завершення академічного семінару, підполковник Цезарі Козловські (Республіка Польща, Центр передового досвіду НАТО в галузі енергетичної безпеки) представив сценарій КШН.

Друга фаза CORE 20 полягала у проведенні дводенних КШН, головної події п'ятиденної програми. Учасники були розподілені по п'яти різних навчальних групах (синдикатах):

(1) Координаторами синдикату (групи) «Захист критичної інфраструктури (ЗКІ) від небезпек, загроз та атак» були доктор Олександр Суходоля (Національний інститут стратегічних досліджень, Україна), пан Павел Каспшик (Республіка Польща, Європейський центр передового досвіду з протидії гібридним загрозам),

(2) Координаторами синдикату (групи) «Кібербезпека» були пан Олександр Бакалинський (Україна, Державна служба спеціального зв'язку та захисту інформації України) та майор Емре Халісдемір (Республіка Туреччина, Центр передового досвіду спільного кіберзахисту НАТО),

(3) Координаторами синдикату (групи) «Морська безпека» були капітан Степан Яким'як (Україна, Національний університет оборони України), капітан Ертюрк Авджі (Республіка Туреччина, Центр передового досвіду НАТО в галузі морської безпеки) і Александру Гудіштяну (Військово-Морські сили Румунії, Центр передового досвіду НАТО в галузі морської безпеки),

(4) Координаторами синдикату (групи) «Стратегічна комунікація (СТРАТКОМ)» були пані Любов Цибульська (Український кризовий медіацентр), полковник Дуглас Кохран (Сполучене Королівство, 1 німецько-нідерландський корпус) і підполковник Енні Гейсоу (Сполучене Королівство, Центр передового досвіду НАТО в галузі стратегічних комунікацій),

(5) Координаторами синдикату (групи) «Міжнародне реагування/Міжнародне право» були доктор Анна Шелест (керівник безпекових програм, Рада зовнішньої політики «Українська призма») та пан Сергій Карасов (компанія «Lano Solutions»).

Третя фаза CORE 20 складалася з Підбиття підсумків КШН (Обговорення результатів) і збігалася з днем високоповажних гостей. На цій фазі доповідачі від кожного синдикату мали можливість коротко викласти оцінку й реагування своєї групи на обрану ввідну, а також висвітлити загальні результати групи щодо виявлених областей для вдосконалення і передового досвіду. Почесні гості склалися зі значної кількості високопоставлених чиновників, дипломатів і представників галузі. Перед учасниками виступила Ольга Стефанішина, Віцепрем'єр-міністр з питань європейської та євроатлантичної інтеграції.

1.2.4. Кінцевий звіт про навчання

Цей звіт в основному зосереджений на реагуванні синдикатів на сценарні епізоди та ввідні, що охоплювали зафіксовані ключові висновки – області для вдосконалення, передовий досвід і рекомендації. У наступному розділі звіту подано сценарій навчань. Наступні розділи містять звіти по кожній навчальній групі (синдикату), в яких наводиться короткий виклад відповідей на кожен епізод і ввідну, а також ключові висновки. З огляду на доречність та/або брак часу кожна група (синдикат) розглядала не кожен ввідну. Крім того, існують деякі відмінності щодо підходів синдикатів у

складанні звітів. У завершальному розділі розглядаються ширші ключові висновки, що стосуються не тільки однієї групи.

Читачі помітять, що навчання базувалися на вигаданому сценарії, який дуже нагадував регіональні реалії, тому сформульовані відповіді навчальних груп відповідали сценарію, але ключові висновки надавалися без посилання на вигадані країни тощо.

Оцінювачі навчань зібрали та надали проекти відповідей і ключових висновків груп, які були розглянуті, уточнені й розширені під час обговорення після навчань, що пройшло в Києві, Україна, 8-9 листопада 2021 року, де зібралися кілька координаторів, учасників і оцінювачів, аби сформулювати більшу частину остаточного тексту цього звіту – це була командна робота.

2. Сценарій Командно-штабних навчань CORE 20

2.1. Передумови і Сценарій

Представлений сценарій взято безпосередньо з документів з планування навчань і було надано учасникам КШН.

2.2. Геополітична ситуація

Геополітична напруженість між двома колишніми країнами імперії Понуксін: Бастаном і Сентою, продовжувала впливати на геополітичну ситуацію в регіоні. Імперські забаганки Бастана стали причинами постійних спроб Бастана дестабілізувати політичну й економічну ситуацію в Сенті. Основною метою дій Бастана було відродження колишньої імперії Понуксін в рамках так званого Союзу об'єднаних держав, де Сента перебувала б під повним управлінням і владою Бастана, оскільки останній встановив би регіональне панування над отриманою територією і ресурсами сусідніх держав. Центральний стратегічний півострів у морі Нуар, що належить Сенті, залишався окупованим Бастаном.



Загальне сприйняття Бастаном ЄС і НАТО було швидше негативним, оскільки розширення ЄС і НАТО підриває плани Бастана щодо регіональної інтеграції. ЄС розглядався як конкурент майбутньому Союзу об'єднаних держав. НАТО розглядалося як агресивна організація, яка усуває режими, що підтримують зусилля Бастана з реінтеграції в Союз об'єднаних держав.

2.3. Соціально-економічна ситуація

Нещодавно в Сенті відбулася проєвропейська маніфестація, а згодом і народна революція, яка скинула корумпованих президента та урядовців, що підтримували політику Бастана. В результаті було обрано новий уряд з чіткими проєвропейськими прагненнями та метою вступити в ЄС і НАТО.

Через попередні політичні потрясіння і високу корупцію економіка Сенти зазнавала труднощів, хоча останні роки показали початок періоду стабілізації. Водночас проблеми, пов'язані з пандемією, сповільнили економічне зростання як в Сенті, так і в інших країнах. Високий рівень безробіття призвів до соціальної напруженості. Зростання кількості протестів на вулицях було викликане відсутністю ефективних реформ в економічній системі, монополізацією енергетичних ринків місцевими олігархами, високим рівнем природних і антропогенних ризиків в результаті зносу критично важливої інфраструктури країни через її тривалий термін експлуатації.

Транспортний сектор Сенти, зокрема його портова галузь, був важливим чинником економічного розвитку країни та воротами зовнішньої торгівлі. Наприклад, 20 відсотків ВВП країни було отримано завдяки портам. У великих морських портах працювало двісті тисяч осіб. Крім того, на порти припадало 70 відсотків експорту Сенти та 65 відсотків її імпорту. Порти Сенти були вкрай важливим елементом логістичної інфраструктури країни, становлячи найпотужніший портовий потенціал серед усіх країн регіону моря Нуар, оскільки майже половина всіх завантажених контейнерів в морі Нуар оброблялася в терміналах Сенти. Тим не менш, дедалі агресивніші дії уряду Бастана в морській сфері порушили ефективне використання портового потенціалу, погіршивши економічну ситуацію.

Імпортний та експортний потенціал енергетичних ресурсів Сенти був пов'язаний з портовою інфраструктурою в південній частині Сенти. Одеський морський порт, а також морський порт «Південний», морські порти Чорноморська і Миколаєва були важливими морськими воротами для постачання енергоносіїв і хімічної продукції в регіоні. Вищезазначені порти також становили істотну частину об'єктів з перевалки та зберігання нафти й газу в Сенті.

Нещодавно було підтверджено наявність значних запасів нафти й газу у ВЕЗ Сенти. Їх розробка могла б забезпечити вищий рівень енергетичної безпеки і стати джерелом стабільного фінансового зростання для Сенти. Крім того, у Сенти є потенціал стати одним з провідних виробників газу й нафти в регіоні. Очікується, що нові ПІІ в секторі видобутку нафти й газу значно зростуть в найближчі кілька років. Великі нафтогазові компанії, як місцеві, так й іноземні, отримали ліцензії та розпочали розвідувальні роботи, плануючи почати буріння нафтових і газових свердловин у ВЕЗ Сенти в морі Нуар.

Більш того, прибережна частина ВЕЗ Сенти в морі Нуар вважалася одним з кращих місць для установки вітрогенераторів.

2.4. Метеорологічна обстановка та ситуація з попитом на газ

Сента пережила одну з найхолодніших зим в історії. Температура трималася незвично низькою вже третій тиждень з середини грудня. Вона постійно залишалася на рівні -20°C , а в деяких районах досягала -35°C . Море Нуар ставало все більш крижаним, особливо вздовж берегової лінії, а морський рух в цих районах був можливим тільки за допомогою буксирів.

Швидкість вітру досягала 40 м/с , в той час, як в деяких районах була зафіксована швидкість 50 м/с . Сильні вітри завадили проведенню перевалки вантажів у Сенті. Поромам довелося довго стояти на рейді, чекаючи поліпшення погоди.

Опалювальний сезон був у самому розпалі. Попит на газ досяг історично високих обсягів, які раніше не спостерігалися у Сенті. Постачальники тепла, які використовували біомасу, перейшли на газ, аби задовольнити попит на тепло в умовах екстремальних холодів.

Попит на газ для внутрішнього споживання, зареєстрований 4 січня, склав 10 млн м^3 на добу в Одеській області та 6 млн м^3 на добу в Миколаївській області. Транзит¹ газу через територію Сенти в сусідні країни здійснювався на повну потужність.

2.5. Безпека критичної інфраструктури в регіоні

Загальна структура виробництва, розподілу і постачання електроенергії в Південному регіоні Сенти була зображена за аналогією з системою реальної країни – України.

Інфраструктура виробництва, постачання і розподілу електроенергії Сенти сформувала об'єднану енергетичну систему (ОЕС) – сукупність електростанцій, електричних мереж, інших об'єктів електроенергетики, об'єднаний штатний режим виробництва, передачі та розподілу електричної енергії з його централізованим управлінням.

ОЕС Сенти забезпечувала надійне та ефективне енергопостачання споживачам по всій країні та за кордоном, підтримуючи високий рівень енергетичної безпеки країни. Безпеку електропостачання в Південному регіоні Сенти забезпечували такі електростанції:

- Південно-Сентська атомна електростанція - 3000 МВт ;
- Дністровська гідроакмулююча електростанція - 972 МВт ;
- Ташлицька гідроакмулююча електростанція - 302 МВт ;
- Одеська теплова електростанція - 68 МВт ;
- Миколаївська теплова електростанція - 40 МВт .

¹ У грудні 2019 року Сента і Бастан підписали новий 5-річний контракт на транзит Бастанського газу через територію Сенти. Згідно з контрактом обсяг транзиту був скорочений до 65 мільярдів кубометрів на рік у 2020 році, а надалі до 40 мільярдів кубометрів на рік у 2021-2024 роках.

Важливо відзначити, що Дністровська гідроакумулююча електростанція покривала 90 відсотків потреб Одеської області.

Одеська та Миколаївська області на півдні Сенти були важливими регіонами транскордонного електропостачання від Бастана до Вели та Румунії через лінії електропередачі з напругою 330 кВ і 400 кВ. Основні лінії енергосистеми між Сентою і Велою поєднувалися за допомогою Молдавської ГРЕС потужністю 2520 МВт, яка розташовувалася на території Вели.

У Південному регіоні Сенти була високо розвинена газова інфраструктура: налічувалося 58 головних газоперекачувальних станцій і 100 вузлів обліку газу. Значення газопостачання в цьому регіоні було високим, оскільки газ використовувався по всій країні у виробництві й промисловості, а також державними закладами. Газ посідав друге місце в списку найбільш споживаних ресурсів впродовж опалювального сезону.

Провідною газотранспортною компанією в Одеській області була «Одесагаз», під управлінням якої знаходилося 440 газоперекачувальних станцій і понад 12 318,6 км газопроводів.

Попри скорочення транзиту природного газу через територію Сенти відповідно до умов нового 5-річного контракту з Бастаном, Південний регіон Сенти залишався важливим для транзиту газу Бастану в Велу та Румунію. Одеська і Миколаївська області були важливими територіями, через які від Бастана до Вели і Румунії проходить Південний газотранспортний трубопровід. Таким чином, Сента відіграла вирішальну роль в постачанні газу в країні ЄС.

Вказані нижче об'єкти були центральними в газотранспортній інфраструктурі Сента-Вела:

- Газокомпресорні станції Березівка, Павлоград і Марівка Південного газотранспортного коридору;
- Міждержавні точки з'єднання: Гребеники, Каушани, Орлівка (розташовані в газовому коридорі Сента-Вела-Румунія на території Сенти).

У ВЕЗ Сенти в морі Нуар були виявлені значні родовища газу. Після геологорозвідувальних робіт в межах залягання родовища було встановлено кілька нових самопідйомних бурових установок: Одеська, Штормова і Галицинська. Однак після захоплення Бастаном нафтових і газових родовищ Сенти в морі Нуар разом з інфраструктурою та обладнанням, що використовувалися для їх розробки і постачання споживачам, ця частина шельфу опинилася під контролем Бастана.

Наявність нових прилеглих нафтогазових районів у межах ВЕЗ Сенти в морі Нуар (район Дельфін) визначило економічну доцільність їх розробки, отримання економічного прибутку та підвищення рівня безпеки енергопостачання Сенти.

Одеса використовувалася як важливий морський транспортний вузол. У місті розташовувалися два склади: «Одеснафтопродукт» і «Ексімнафтопродукт».

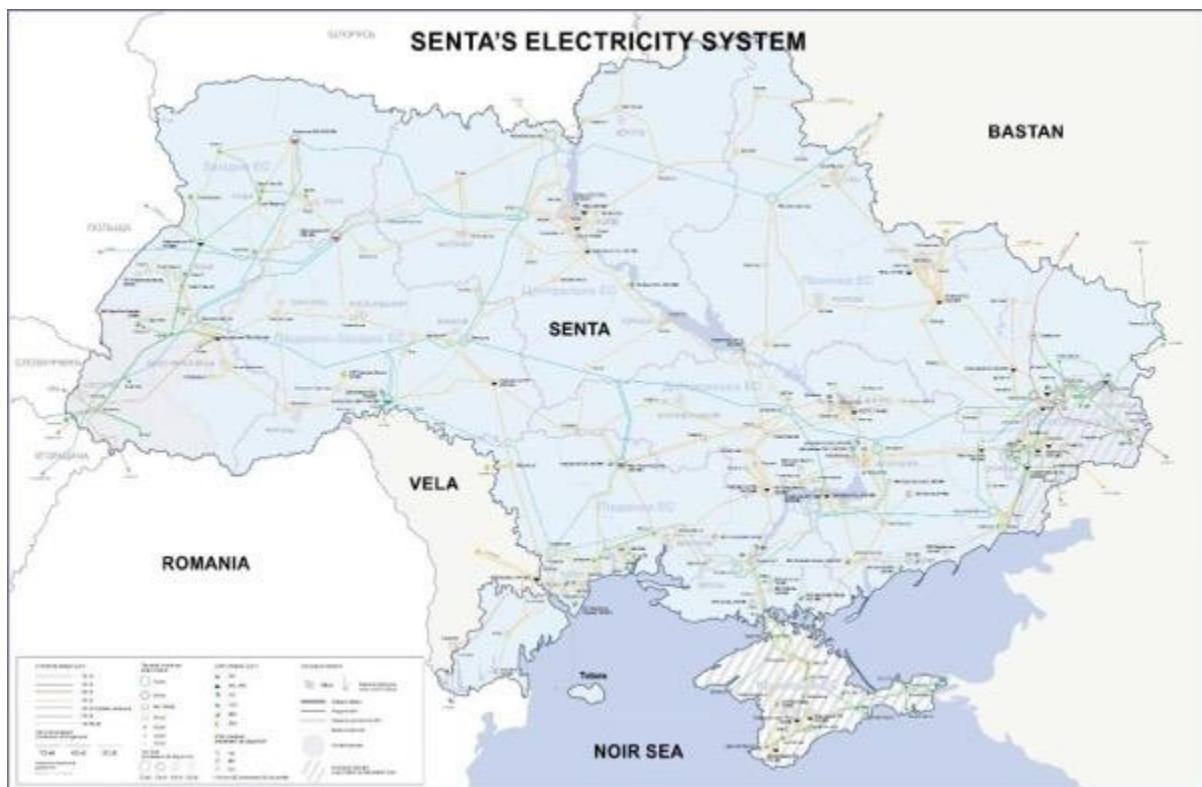
Морські порти Сенти були центральною частиною перевалочної інфраструктури держави. Основні судноплавні лінії проходили через Одеський морський порт, Миколаївський морський порт, морський порт «Південний» і Чорноморський морський порт. Провідна інфраструктура з перевалки та зберігання нафти, газу та хімічних продуктів була розташована в таких портах:

- Одеський морський порт – морський нафтогазовий термінал;

- Морський порт «Південний» – база з перевалки аміачного газу, морський нафтовий термінал «Південний» (Укртранснафта), приватні термінали, в тому числі компанії «TIS»;
- Миколаївський морський порт – база з перевалки вугілля і нафти;
- Чорноморський морський порт – морський нафтогазовий термінал, цех з перероблення сірки.

Морські порти Сенти відігравали вирішальну роль у перевалці вантажів і пересадці пасажирів між Сентою та іншими сусідніми державами. Саме в Одеських портах відбувається перевалка металопродукції Сенти. Минулого року вантажообіг Одеського морського порту досяг показника у 25 343 млн т. Крім того, порти Одеської області є центральними пунктами для експортних перевалок зернових, руд, корисних копалин, вугілля і чавуну.

У безпосередній близькості від південно-західного узбережжя знаходився Острів Тотара з населенням приблизно 12500 жителів, що проживають в трьох основних поселеннях. На острові був морський порт і три бурові установки. З континентальною частиною Сенти Острів Тотара був з'єднаний підводним інтернет-кабелем Сента-Тотара-Болгарія, який був основним джерелом Інтернету для всього острова Тотара. У водах навколо Острова Тотара знаходилося вісім газових і чотири нафтових самопідійомних бурових установки, в тому числі ті, що захоплені Бастаном та контролюються ним.



2.6. Ситуація з морською безпекою

Останнім часом загальна ситуація з морською безпекою на морі Нуар погіршувалася. Домінування Бастана в морі Нуар посилювалося. Бастан здійснив швидке нарощування бойових і правоохоронних

спроможностей і почав розміщувати нові та передові надводні бойові кораблі й підводні човни у складі Нуарморського флоту. Тим часом на континентальному шельфі Сенти спостерігалось масове нарощування крилатих ракет протиповітряної та берегової оборони, а також підвищення потенціалу Бастана у сфері радіоелектронної боротьби.

Уряд Бастана неодноразово заявляв, що ширина ВЕЗ Сенти була виміряна неправильно відповідно до положень Конвенції ООН з морського права, оскільки великі райони у вищезгаданій морській зоні були історичними водами Бастана і повинні були б повністю перебувати під його імперативною юрисдикцією. Спірні області позначені на карті нижче.



2.7. Кібербезпека і радіоелектронна боротьба

Загальна ситуація з кібербезпекою досить ворожа. Надходили повідомлення про численні кібератаки у морській сфері та у сфері критичної інфраструктури. Більш того, сайти урядових установ, банків і провідних новинних сайтів працюють з періодичними зривами у роботі. Бастан проводить технічну розвідку інформаційних систем Сенти для збору інформації про вразливості загальнодоступних і корпоративних користувацьких систем Сенти, які можуть бути використані для злочину, шпигунства і диверсій.

Крім того, більшість інформаційних операцій в кіберпросторі націлені на національну систему оборони. Ці атаки спрямовані на поляризацію суспільства, дискредитацію Збройних сил Сенти та зниження довіри до державних інститутів. Крім того, зростає кількість атак програм-вимагачів на державні установи Сенти, а також на приватні та державні компанії.

Найбільша загроза для руйнування критичної інфраструктури Сенти йде від кібератак на автоматизовані системи управління (АСУ), в тому числі в енергетичному та транспортному секторах.

Згідно з оцінкою національної безпеки Сенти спецслужби Бастана особливо активні в спробах отримати доступ і створити загрозу для об'єктів критичної інфраструктури. Ця інформація відповідає нещодавнім повідомленням міжнародних компаній з кібербезпеки, які почали виявляти ознаки нової шкідливої програми для кібератак з кодовою назвою «Blackout», спеціально розробленої для захоплення контролю над енергетичними системами. «Blackout» – це модифікована версія шкідливого програмного забезпечення «Industroyer», вперше виявлена у 2015 році, яка була розроблена для атаки на електроенергетичні системи управління і, як вважають, вона стоїть за кібератакою на електромережу Сенти у 2016 році. Експерти відзначали здатність «Blackout» не тільки залишатися в системі та втручатися в роботу автоматизованих систем управління, але і ставити під загрозу автоматизовані системи безпеки (АСБ), що робить цю програму однією з найнебезпечніших нових шкідливих загроз для автоматизованих систем управління з часів «Stuxnet».

У регіоні зростає кількість інцидентів, пов'язаних з радіоелектронною боротьбою (далі – РЕБ). В останні роки Бастан вклав значні кошти у розбудову спроможностей РЕБ у регіоні моря Нуар. Ці спроможності часто використовують військові та цивільні судна Бастана. Надходили повідомлення про частіші проблеми з супутниковою навігацією у деяких цивільних і військових суден, у тому числі від великих нафтових танкерів у морі Нуар, що наводить на думку про перешкоди й підміну сигналів GPS. Крім того, під час останніх військово-морських навчань Бастана супутниковий зв'язок і система зв'язку в південних районах Сенти відчували перебої.

2.8. Комунікація та повідомлення засобів масової інформації

Інформаційне середовище постійно вороже і знаходиться під істотним контролем Бастана. Триває кампанія з поширення пропаганди та дезінформації, фальсифікації новин інформаційними агентствами та засобами масової інформації Бастана проти Сенти. Мета полягає в тому, аби зганьбити державність Сенти, дискредитувати та розповсюдити дезінформацію про уряд, маніпулювати історією та міжнародно-правовими положеннями стосовно ситуації в морських зонах Сенти.

З цією метою Бастан використовує доступні канали комунікацій, у тому числі інформаційні канали Сенти, контрольовані суб'єктами, яких підтримує Бастан. Це перешкоджає поширенню офіційної проєвропейської позиції уряду Сенти.

Дезінформаційна діяльність Бастана спрямована на зниження рівня підтримки населенням економічних і енергетичних реформ Сенти. Крім того, пропаганда Бастана створює картинку і намагається переконати націю Сента в перевагах членства в Союзі об'єднаних держав, де Бастан заявляє, що це принесе економічний прогрес у порівнянні з членством в ЄС і НАТО.

Операції з перекручування й спотворення інформації в кіберпросторі націлені на урядові установи та приватні компанії Сенти. Ці атаки спрямовані на поляризацію суспільства, дискредитацію Збройних сил Сенти та зниження довіри до державних інститутів. Творці фальшивих історій прагнуть бути більш переконливими та використовують розповіді, які все частіше засновані на реальних подіях. Ці наративи більш широко поширюються в зарубіжних ЗМІ; залучаються нові інститути та соціальні групи, що сприяє поширенню дезінформації.

Ситуація зі свободою слова на окупованій території Сенти є принизливою. У ЗМІ регулярно з'являються повідомлення про порушення прав людини та придушення виступів громадських активістів силами Бастанана.

2.9. Висновки щодо сценарію

Представлений у цьому документі сценарій обговорювався під час семінарів з обговорення сценарію, епізодів та ввідних, що відбулися у жовтні 2019 року та травні 2021 року в Києві, Україна. Він був розглянутий, обговорений і остаточно прийнятий зацікавленими сторонами.

Цей сценарій був використаний для розробки епізодів та ввідних для КШН CORE 20.

2.10. Розділ про епізоди та ввідні

Було сформовано п'ять окремих навчальних груп (Синдикатів) і, відповідно, кожна Група проходила свої власні командно-штабні навчання з невеликими відмінностями у ввідних, включених у сценарій. У кожній з п'яти груп були представники різних міністерств, безпекових організацій та енергетичної галузі, що було необхідно для сприяння в їх аналізі за пріоритетними напрямками. Були такі Навчальні групи (Синдикати): 1. ЗКІ від небезпек, загроз та атак, 2. Кібербезпека, 3. Морська безпека, 4. Стратегічні комунікації (СТРАТКОМ), 5. Міжнародне реагування/Міжнародне право.

Навчання проводилися з огляду на гібридні загрози, які формують передумови для розвитку сценарію. Це охоплює важливі компоненти безпеки постачання електроенергії та природного газу у вигляді перебоїв у постачанні, кібератак і нападів з використанням електронних засобів на критично важливу інфраструктуру, морські загрози судноплавству і портовій інфраструктурі. Також розглядалося поєднання соціально-економічних, геополітичних елементів та елементів стратегічної комунікації.

У цьому документі представлені епізоди та ввідні для КШН CORE20, що ґрунтуються на сценарії.

Хронологія розвитку кризи:

- криза починається 6 січня 20XX-го року, об 11:00;
- за сценарієм криза триває впродовж восьми тижнів до 6 березня.

2.11. Структура епізодів та ввідних

Що таке епізод? Як правило, епізоди надають загальний огляд, що описує інцидент, який використовується для ілюстрації або ідентифікації конкретної проблеми. Епізод - це короткий опис, розповідь або подія, що викликає сильні образи, спогади або почуття. Командно-штабні навчання на основі епізоду - це навчання, в яких детальна інформація з епізоду використовується як ввідні дані та обстановка навчань. Іншими словами, це інцидент з відносно великими наслідками, який вимагає реакції з боку учасників.

Що таке ввідна? Ввідна - це коротка історія події, яка використовується для залучення уваги гравців до інциденту, вона була створена для цих гравців (і від них очікується реакція). Іншими словами, це інцидент з відносно невеликими й локальними наслідками, який вимагає реакції від вибраної частини учасників. Різні ввідні можуть використовуватися в рамках одного і того ж епізоду для різних дискусійних груп (що також іменуються синдикатами).

Навчальна група опрацюватиме п'ять епізодів для кожної фази сценарію і кілька ввідних для кожного епізоду:

Епізод 1: Доконфліктна фаза: Гібридний вплив

Посилюється політичне та економічне залякування з боку влади Бастана. Ґрунтуючись на угоді про транзит газу, яка була підписана між Бастаном і Сентою минулого року, уряд Бастана звинуватив Сенту в порушенні положень угоди. Сента заперечує будь-які порушення. Однак ЗМІ Бастана і деякі ЗМІ Сенти, контрольовані Бастаном, продовжують поширювати повідомлення про порушення Сенти, підкреслюючи важливість відповідної угоди для енергетичної безпеки Європи, оскільки транзит газу² в європейські країни частково забезпечується через територію Сенти.

Ситуацію ускладнює той факт, що між Бастаном і Велою не укладено новий контракт на постачання газу. Враховуючи суперечки щодо договірних положень, Бастан тимчасово істотно скорочує постачання газу у Велу. Вела максимально відбирає газ з транзитного трубопроводу, обмежуючи постачання газу споживачам Сенти в Одеській області, недалеко від кордону з Румунією.

Тим часом Бастан ввів обмеження на імпорт товарів сільського господарства, обробної промисловості та металевих виробів Сенти, а також палива, хімікатів і нафтопродуктів. Крім того, Бастан припиняє постачати нафтопродукти в Сенту автомобільним, залізничним транспортом і трубопроводами.

В Інтернеті були виявлені три вебсайти з ідентичним візуальним оформленням і функціями офіційних вебсайтів Оператора ГТС Сенти, Оператора PSG і компанії «Нафтогаз». Крім того, на електронні адреси регіональних урядових установ Сенти були надіслані листи з фішинговими функціями та прикріплені текстові документи Microsoft Word.

У ЗМІ з'явилися повідомлення про потужну кібератаку на внутрішню мережу Liebherr в Німеччині. В результаті портові крани в морському порту Поті в Зестані перестали працювати.

З середини грудня берегова охорона Сенти регулярно повідомляє про присутність Військово-морських сил Бастана у ВЕЗ Сенти. Повідомляється, що Бастан проводив військові навчання в морі Нуар у безпосередній близькості від фарватерного проходу торгових і пасажирських суден з/в порти Одеської області.

Епізод 2: Гібридні операції низької інтенсивності

² Завершення нових проєктів газової інфраструктури впродовж останніх років дозволяє Бастану переорієнтувати більшу частину постачання газу в країни Центральної та Південно-Східної Європи без використання транзитного коридору Сенти.

На початку лютого погодні умови в південних районах Сенти погіршилися. Швидкість вітру досягає 50 м/с, що завдає значної шкоди, зокрема, в Одеській області.

Введені Бастаном обмеження на імпорт товарів сільського господарства, обробної промисловості та металевих виробів, палива, хімікатів і нафтопродуктів із Сенти сприяють занепаду економіки Сенти, яка вже знаходиться в стані рецесії. Пробастанські активісти використовують економічний спад як шанс посилити протести проти уряду Сенти. Соціальна напруженість досягає свого піка, коли в Інтернеті поширилася новина про рішення Одеської міської ради про вихід Одеської області зі складу Сенти.

Діяльність пробастанських активістів та інцидентами у сфері кібербезпеки постійно порушують роботу Одеського морського порту. Крім того, цивільні судна і кораблі берегової охорони Сенти повідомляли про технічні неполадки у роботі своїх навігаційних систем.

Крім того, судна Бастана діють агресивно проти риболовецьких суден Сенти. Кораблі берегової охорони Бастана залякують і погрожують вантажним суднам Сенти, а також суднам іноземних держав. Нещодавно Військово-морські сили Бастана надали підтримку незаконній діяльності з розвідки газу та встановлення бурових установок на території ВЕЗ Сенти. Навколо бурових установок був встановлений цілодобовий охоронний патруль Військово-морських сил Бастана.

Епізод 3: Фаза конфлікту: Гібридні операції високої інтенсивності

Критична інфраструктура Сенти піддається широкому спектру ударів кінетичною і некінетичною зброєю. Перебої в роботі газопроводу з транспортування природного газу через південний газотранспортний коридор позначаються на постачаннях газу в південний регіон Сенти та сусідні краї. Більш того, існує загроза зриву опалювального сезону не лише в південній частині Сенти, але й у Харківській і Луганській областях, які, зокрема, сильно залежать від постачання газу з Бастана.

На півдні Сенти на третину збільшилася кількість надзвичайних ситуацій, пожеж і нещасних випадків, викликаних підпалами й терористичними актами з використанням вибухових речовин, що призвело до значного збільшення числа постраждалих. Є підозра про масштабний інцидент на ПАТ «Одеський припортовий завод», де повідомляється про значний викид небезпечних хімічних речовин.

Поширюється інформація про перебої в роботі Південно-Сентської АЕС. ЗМІ Бастана звинувачують владу Сенти у викидах радіації. Майже одночасно поширюється інформація про атаку на гідро-акумуляуючу електростанцію.

Масовані кібератаки порушують роботу Одеського морського порту, в тому числі транспортування й обробку вантажів. Нападу зазнали банківські системи відділень Ощадбанку і ПриватБанку в Одеській області.

Через місяць після першої кібератаки на внутрішню мережу Liebherr в Німеччині сталася серія незначних кібератак на портові крани Liebherr по всій Європі.

У морській сфері кораблі ВМС Бастана збільшують свою присутність у ВЕЗ Сенти, використовуючи Військово-морські навчання, припиняючи міжнародні морські перевезення пасажирів і вантажів.

Епізод 4: Гібридна війна

Напруженість у відносинах між Бастаном і Сентою досягла найвищого рівня за всю їх історію. Військова розвідка Сенти повідомила про безпрецедентне нарощування військових сил і засобів на базах Бастанського флоту в морі Нуар. На острові Тотара почала відбуватися значна кількість провокаційних нещасних випадків. Повідомлення про втрату сигналів GPS і GSM на острові. Підключення до Інтернету на острові зникло.

У той самий час Сента продовжує стикатися зі збільшенням кількості кібератак на урядові та місцеві установи та постачальників критично важливих послуг. ЗМІ Бастана і Сенти повідомляють в агресивній манері про нездатність центральної та місцевої влади Сенти надавати населенню основні послуги. Більш того, вищі командири Збройних сил Сенти в Києві та посадові особи Військово-морських сил в Одесі та на острові Тотара отримали електронні листи з непідтверджених профілів з прямим попередженням «не виконувати накази політичного керівництва Сенти, інакше вони та їхні сім'ї будуть у небезпеці».

Соціальні мережі сповнені повідомлень і активних дискусій про можливе відділення південної частини Сенти. Ті ж новини поширюються через офіційні вебсторінки регіональних рад. Все вищевказане призводить до тиску всередині державних установ, правоохоронних органів і збройних сил. За останні 24 години різко посилюються вуличні демонстрації проти уряду Сенти, а саме в центральних містах південних регіонів: Одесі, Миколаєві та Херсоні. В результаті уряд функціонує на межі можливого, а населення збентежене.

На тлі значних кібератак, психологічного тиску, поширення дезінформації і дедалі більших вуличних протестів у південних регіонах на острові Тотара раптово висадилася значна кількість о/с збройних сил без розпізнавальних знаків. Доступ до порту острова Тотара заблокований вантажними суднами без розпізнавальних знаків і прапора держави. Доступ по воді до острова Тотара відрізаний. Бурові установки для видобутку вуглеводнів на острові Тотара, розташовані у ВЕЗ Сента, були захоплені й тепер знаходяться під повним контролем озброєних людей без розпізнавальних знаків.

Епізод 5: Посткризова стабілізація

Цей епізод був присвячений посткризовому відновленню та процесу стабілізації. Посткризова стабілізація відбувається після закінчення кризового сценарію – з 7 березня 20XX року. Також потрібно обговорити питання управління в кризових ситуаціях.

Примітки до епізоду

Кожному синдикату буде запропоновано кілька питань для обговорення посткризової стабілізації. Епізоди 1 - 4 містять ввідні для кожного з п'яти синдикатів. Епізод 5 відображає питання для обговорення для кожного з п'яти синдикатів.

Всі події тривають 59 днів, з 6 січня по 5 березня (Доконфліктна фаза триває 21 день, Гібридні операції низької інтенсивності тривають 28 днів, фаза конфлікту триває шість днів, а гібридна війна триває чотири дні).

Ввідні згруповані для кожного з 5 синдикатів:

Синдикат (Група) 1 – ЗКІ від небезпек, загроз і атак

Синдикат (Група) 2 – Кібербезпека;

Синдикат (Група) 3 – Морська безпека;

Синдикат (Група) 4 – СТРАТКОМ;

Синдикат (Група) 5 – Міжнародне реагування/Міжнародне право.

Навчальним групам усіх синдикатів були надані сценарій, епізоди та ввідні, а також окремо надрукована мапа системи електропостачання Сенти. Синдикат 3 (Морська безпека) був додатково оснащений чотирма морськими картами (по одній для кожного епізоду 1 - 4) з точним зазначенням місць подій.

3. Синдикат (Група) 1: ЗКІ від небезпек, загроз і атак



Національний інститут стратегічних досліджень України, доктор Олександр Суходоля, координував роботу Синдикату з реагування на кризи і представляє Епізод під час проведення КШН CORE 20 в Одесі, Україна.

3.1. Епізод 1: Доконфліктна фаза: Гібридний вплив

Посилюється політичне й економічне залякування з боку влади Бастану. На підставі угоди про транзит газу, яка була підписана між Бастаном і Сентою минулого року, уряд Бастану звинуватив Сенту в порушенні положень угоди. Сента заперечує будь-які порушення. Однак ЗМІ Бастану і деякі ЗМІ Сенти, контрольовані Бастаном, продовжують поширювати повідомлення про порушення Сенти, підкреслюючи важливість відповідної угоди для енергетичної безпеки Європи, оскільки транзит газу в європейські країни частково забезпечується через територію Сенти.

Ситуацію ускладнює той факт, що між Бастаном і Велою не укладено новий контракт на постачання газу. Враховуючи суперечки щодо договірних положень, Бастан тимчасово скорочує постачання газу в Велу. Вела максимально відбирає газ з транзитного трубопроводу, обмежуючи постачання газу споживачам Сенти в Одеській області, недалеко від кордону з Румунією.

Тим часом Бастан ввів обмеження на імпорт сільськогосподарських, промислових товарів і металевих виробів, палива, хімікатів і нафтопродуктів із Сенти. Крім того, Бастан припиняє постачати нафтопродукти в Сенту автомобільним, залізничним транспортом і трубопроводами.

В Інтернеті були виявлені три вебсайти з ідентичним візуальним оформленням і функціями офіційних вебсайтів Оператора ГТС Сенти, Оператора PSG і компанії «Нафтогаз». Крім того, на

електронні адреси регіональних урядових установ Сенти були надіслані листи з фішинговими функціями та прикріплені текстові документи Microsoft Word.

У ЗМІ з'явилися повідомлення про потужну кібератаку на внутрішню мережу Liebherr в Німеччині. В результаті портові крани в морському порту Поті в Зестані перестали працювати. З середини грудня берегова охорона Сенти регулярно повідомляє про присутність Військово-морських сил Бастана у ВЕЗ Сенти. Повідомляється, що Бастан проводив військові навчання в морі Нуар у безпосередній близькості від фарватерного проходу торгових і пасажирських суден з/в порти Одеської області.

Ввідна 1.1.1: День 1: 6 січня, 11:00

Через рік після підписання угоди про транзит газу влада Бастана звинувачує Сенту в порушенні угоди, попереджаючи про розірвання контракту і припинення постачання газу через територію Сенти.

Реагування на Ввідну 1.1.1

Головною турботою учасників була здатність країни забезпечити достатнє газопостачання для організації зимового опалення. Велися широкі дискусії про те, як різні рівні державних структур будуть реагувати на цю загрозу, але було неясно, яке конкретне міністерство або комісія візьмуть на себе провідну роль у розв'язанні цієї проблеми. Лідер синдикату був непохитний у тому, що це питання має політичний характер і вимагатиме дій від Кабінету Міністрів. Обговорювалися альтернативні шляхи енергопостачання; однак було неясно, які дії можна зробити для усунення потенційного дефіциту енергопостачання. Синдикат погодився з тим, що найбільш розсудливим варіантом розвитку подій було б скликання призначеної Міжвідомчої військової групи, схваленої центральною владою, для оцінки загрози та розробки заходів реагування.

Ввідна 1.1.2: День 9: 14 січня, 13:00

Бастан оголошує про блокування експорту антрацитового вугілля з Бастану і східної частини Сенти (окупована територія, непідконтрольна уряду Сенти) в Сенту, а також забороняє імпорт сільськогосподарської продукції, металу, чорних і кольорових металів, хімікатів, обладнання, палива і нафтопродуктів з Сенти, посилаючись на гадані грубі порушення вимоги до якості товарів.

Реагування на Ввідну 1.1.2

Ця ввідна викликала широке обговорення наслідків блокування Бастаном імпорту вугілля і введення обмежень на експорт Сенти. Обговорення включало: альтернативні джерела енергії (економія ресурсів, доступні резерви); масові заворушення через перебої в постачанні; можливість проведення Бастаном кампанії з дезінформації, спрямованої на підрив діяльності уряду Сенти; очевидна відсутність механізмів координації дій щодо реагування державного і приватного секторів з метою зниження наслідків і, що найбільш важливо, відсутність набору взаємопов'язаних, сумісних, концептуальних, законодавчих і нормативних планів і регламентів, які забезпечують системний підхід до планування на всіх рівнях управління, для усіх юрисдикцій та усіх категорій зацікавлених сторін, що беруть участь у реагуванні на інциденти та кризові ситуації, які виникають в результаті будь-яких загроз і небезпек.

Учасники також провели розширене обговорення, що стосувалося виявлення та захисту критично важливої інфраструктури. Було запропоновано скласти список об'єктів (стратегічних активів), визначених національним урядом, які становлять критичну інфраструктуру на місцевому, регіональному та національному рівнях. Обговорювалося, що війська, поліція і національна гвардія несуть відповідальність за захист стратегічних активів, проте не обговорювалися деталі того, якою буде роль інших служб швидкого реагування в цьому відношенні. У коментарях дослідження вказані

кілька відомств, яким відводиться роль захисту критичної інфраструктури. Учасникам було зрозуміло, що поточна ситуація в Україні стосовно захисту критичної інфраструктури відноситься виключно до місії та обов'язків кожного відомства, що робить практично неможливими єдині дії на національному рівні.

Відна 1.1.3: День 15: 20 січня, 10:00

Частково виведено з ладу телекомунікаційне обладнання (комутатори на розподільній станції постачальника послуг у морському порту в Одесі), тимчасова відсутність зв'язку з об'єктами критичної інфраструктури. Переведення на резервну систему електропостачання.



Реагування на Ввідну 1.1.3

Як національний пріоритет була визначена необхідність відновлення телекомунікаційного зв'язку. З метою зменшення наслідків втрати зв'язку негайним реагуванням учасників було використання Збройних сил Сенти для вирішення ситуації, що погіршується. Учасники обговорили питання, що у Сенти немає комплексної бази даних для ідентифікації та класифікації критичної інфраструктури. В ході обговорення виникли побоювання, що для підтримки функціонування критичної інфраструктури буде потрібен перехід на альтернативний ланцюжок постачання, проте було неясно, який державний орган володіє повноваженнями або потенціалом для розгортання резервних

генераторів. Також стало очевидним, що у Сенти немає комплексної бази даних для ідентифікації та класифікації критично важливої інфраструктури.

Були проведені дискусії про роль та обов'язки урядових структур. Було запропоновано створити комісію на державному рівні за участю представників відповідних міністерств для вирішення цієї ситуації. Прем'єр-міністр скликає Комісію з питань техногенно-екологічної безпеки і надзвичайних ситуацій для аналізу ситуації, оцінки та прийняття рішень щодо процедур зниження наслідків, розподілу обов'язків і визначення пріоритетних дій. Ця організація фінансується і має штатний персонал, призначений відповідними міністерствами. У міру того, як учасники продовжували обговорювати варіанти реагування на інциденти, стало зрозумілим, що єдність дій буде залежати від вичерпного набору планів реагування на надзвичайні та кризові ситуації, чого у Сенти не було. Також було виявлено необхідність обміну інформацією на всіх рівнях і серед державних структур, а також в межах секторів критичної інфраструктури, що зазнали впливу.

Учасники погодилися з тим, що визначення характеру загрози має вирішальне значення для прийняття рішення про належне реагування. Ключовим було те, що порушення в роботі віднесені до кампанії з гібридного впливу з боку Бастана.

3.2. Епізод 2: Гібридні операції низької інтенсивності

На початку лютого погодні умови в південних районах Сенти погіршилися. Швидкість вітру досягає 50 м/с, що завдає значної шкоди, зокрема, в Одеській області.

Введені Бастаном обмеження на імпорт товарів сільського господарства, обробної промисловості та металевих виробів, палива, хімікатів і нафтопродуктів із Сенти сприяють занепаду економіки Сенти, яка вже знаходиться в стані рецесії. Пробастанські активісти використовують економічний спад як шанс посилити протести проти уряду Сенти. Соціальна напруженість досягла свого піка, коли в Інтернеті поширилася новина про рішення Одеської міської ради про вихід Одеської області зі складу Сенти.

Діяльність пробастанських активістів та інциденти у сфері кібербезпеки постійно порушують роботу Одеського морського порту. Крім того, цивільні судна і кораблі берегової охорони Сенти повідомляли про технічні неполадки у роботі своїх навігаційних систем.

Крім того, судна Бастана діють агресивно проти риболовецьких суден Сенти. Кораблі берегової охорони Бастана залякують і погрожують вантажним суднам Сенти, а також суднам іноземних держав. Нещодавно Військово-морські сили Бастана надали підтримку незаконній діяльності з розвідки газу та встановлення бурових установок на території ВЕЗ Сенти. Навколо бурових установок був встановлений цілодобовий охоронний патруль Військово-морських сил Бастана.

Реагування на Епізод 2

Було тривале обговорення питання про відповідальність за ці дії й про те, чи така ситуація призводить до оголошення надзвичайного стану або воєнного стану. Представник Державної служби спеціального зв'язку та захисту інформації заявив, що існує необхідність у стратегічних комунікаціях з місцевим населенням щодо дій уряду стосовно стримування кризової ситуації, що розвивається, а також є проблема з випередженням засобів масової інформації щодо висвітлення ситуації для запобігання паніки й масових заворушень.

Учасники також зазначили, що для розв'язання ситуації будуть сформовані комісії на місцевому та регіональному рівнях. Ці комісії консультуватимуть Державну комісію, очолювану Прем'єр-міністром. Один учасник охарактеризував поточний процес прийняття рішень як дуже повільний і централізований. Представники місцевої адміністрації були впевнені, що у них є ресурси та спроможності для реагування на вибух і пожежу, описані у Ввідній 2.

Значну кількість часу було витрачено на обговорення необхідності введення воєнного стану. Висловлювалися побоювання, що оголошення воєнного стану може призвести до подальших масових заворушень. Представники державних служб з надзвичайних ситуацій заявили, що існують плани, укази та постанови для боротьби з надзвичайною ситуацією, але без конкретних подробиць.

Оскільки інциденти торкнулися декількох секторів інфраструктури, учасники не були впевнені, яка гілка влади буде відповідати за управління загальним реагуванням. Крім того, учасники висловили стурбованість тим, що, можливо, не буде достатніх ресурсів або планів для розв'язання проблеми нестачі продовольства, води та енергії. Відбулося поглиблене обговорення питання про резервні фонди для фінансування заходів з реагування в Одеській області. Учасники не були впевнені в тому, як буде здійснюватися запит на виділення і розподіл коштів. Вони вирішили, що запит буде представлений на регіональному рівні для його розгляду спеціальною комісією.

Учасники визначили, що для сприяння міжвідомчій координації потрібні співробітники-координатори, але немає підготовки для виконання конкретних обов'язків такими координаторами. Було відзначено, що українські сили територіальної оборони могли б надавати гуманітарну допомогу, проводити керовані військові, цивільні дії всередині країни та реалізувати програми підтримки цивільної влади щодо оборони, а також надавати підтримку діям цивільної адміністрації.

Ввідна 2.1.1: День 22: 27 січня, 8:00

Під приводом погіршення економічної ситуації та зростання цін на нафтопродукти й паливо прорадянські активісти починають блокувати основні дороги, портові об'єкти та паливні термінали в Одеському морському порту. Невідомі особи перерізали портові телекомунікаційні кабелі на спеціальній кабельній мережі зв'язку за межами території Одеського морського порту.

Реагування на Ввідну 2.1.1

Для розв'язання проблеми з перерізними телекомунікаційними кабелями, учасники визначили, що спеціальні телекомунікаційні служби Одеси (в кожному регіоні є такі служби, які підпорядковуються Державній службі спеціального зв'язку) відреагують на ситуацію з ремонту кабелів і відновлення телекомунікаційних послуг.

Поліція очолить відповідні дії з відновлення порядку за підтримки Національної гвардії. Ця підтримка не вимагає спеціального схвалення на національному рівні. Існує нормативна база, що дозволяє негайно здійснювати цю підтримку, проте військовим потрібен спеціальний дозвіл для отримання підтримки Національної гвардії. У цій ситуації військові також були б приведені в бойову готовність.

Ввідна 2.1.2: День 26: 31 Січня, 12:00

Чути вибух на нафтоховищі Одеського морського порту. Слідом за вибухом на території нафтоховища ОМТП спалахує велика пожежа. Повідомляється про декількох постраждалих. Причина вибуху не підтверджена.

Реагування на Ввідну 2.1.2

Служба пожежної безпеки порту буде першим підрозділом, який відреагує й оцінить необхідну підтримку для гасіння пожежі й відновлення пошкоджених об'єктів. Буде повідомлена Державна служба з надзвичайних ситуацій, а регіональні департаменти також забезпечать медичну й пожежну підтримку. Поліція оточить цей район і забезпечить безпеку.

Реагуванням Антитерористичного підрозділу Служби Безпеки України буде проведення розслідування. Якщо буде встановлено, що це був теракт, то він потрапить під юрисдикцію Служб Безпеки для подальшого реагування. Для цієї ввідної існують відповідні плани, регламенти й процедури, що забезпечують всебічне й ефективне реагування.

Ввідна 2.1.3: День 28: 2 лютого, 03:00

В Одеській області відбувається незначне відключення електроенергії. Початкова оцінка підтверджує, що трансформатори декількох підстанцій фізично пошкоджені. За неперевіреними повідомленнями, по сусідству було чуто кілька пострілів.

Реагування на Ввідну 2.1.3

Учасники заявили, що технічні фахівці будуть реагувати на ситуацію з підстанціями та намагатимуться відновити електропостачання. У разі масштабних дій в Одеській області може бути оголошено надзвичайний стан, і будуть реагувати поліція і національна гвардія. Служба Безпеки також відреагує щодо проведення розслідування.

Регіональна комісія з техногенно-екологічної безпеки і надзвичайних ситуацій, очолювана губернатором Одеської області, проведе екстрену нараду у зв'язку з інцидентом, аби визначити подальші потреби в реагуванні та забезпеченні.

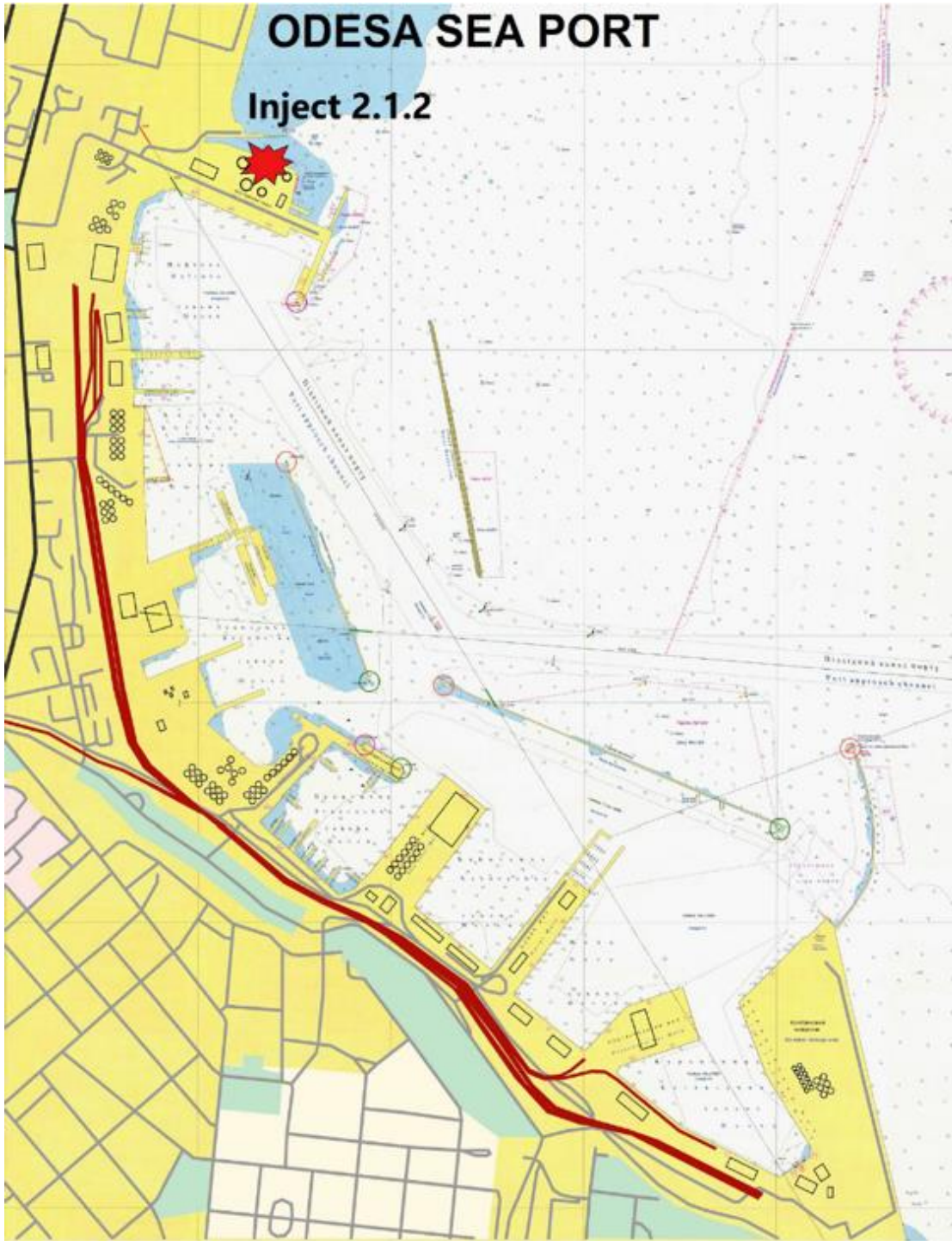
Ввідна 2.1.4: День 36: 10 лютого, 11:00

Високі рівні органічного хлориду забруднюють нафту в трубопроводі «Південна дружба» біля Бродів. Бастан звинувачує Сенту в навмисному акті диверсії. Враховуючи з'єднання трубопроводу «Дружба» з терміналом «Південний» через Одеса-Броди, постачання нафти через цей термінал зазнало істотного впливу.

Реагування на Ввідну 2.1.4

Учасники підкреслили, що забруднити нафту неможливо, адже якщо щось станеться, то оператор побачить це миттєво, і це буде відповідальністю «Укренерго».





3.3. Епізод 3: Фаза конфлікту: Гібридні операції високої інтенсивності

Критична інфраструктура Сенти піддається широкому спектру ударів кінетичною і некінетичною зброєю. Перебої в роботі газопроводу з транспортування природного газу через південний газотранспортний коридор позначаються на постачаннях газу в Південний регіон Сенти та сусідні іноземні держави. Більш того, існує загроза зриву опалювального сезону не лише в південній частині Сенти, але й у Харківській і Луганській областях, які, зокрема, сильно залежать від постачання газу з Бастана.

На півдні Сенти на третину збільшилася кількість надзвичайних ситуацій, пожеж і нещасних випадків, викликаних підпалами й терористичними актами з використанням вибухових речовин, що, своєю чергою, призвело до значного збільшення числа постраждалих. Є підозра про масштабний інцидент на ПАТ «Одеський припортовий завод», де повідомляється про значний викид небезпечних хімічних речовин.

Поширюється інформація про перебої в роботі Південно-Сентської АЕС. ЗМІ Бастана звинувачують владу Сенти у викидах радіації. Майже одночасно поширюється інформація про атаку на гідроакумулюючу електростанцію.

Масовані кібератаки порушують роботу Одеського морського порту, в тому числі транспортування й обробку вантажів. Нападу зазнали банківські системи відділень Ощадбанку і ПриватБанку в Одеській області.

Через місяць після першої кібератаки на внутрішню мережу Liebherr в Німеччині сталася серія незначних кібератак на портові крани Liebherr по всій Європі.

У морській сфері кораблі ВМС Бастана збільшують свою присутність у ВЕЗ Сенти, використовуючи Військово-морські навчання, припиняючи міжнародні морські перевезення пасажирів і вантажів.

Реагування на Епізод 3

Представники ОГТС відзначили, що існують технічні СОП для реагування на перепади тиску газу і що вони успішно використовувалися в реальних ситуаціях. Були дебати щодо органів у сфері реагування на інциденти та відповідальності за пожежі та інциденти з небезпечними речовинами. Крім того, представники місцевої адміністрації, мабуть, були впевнені, що зможуть впоратися з тактичною ситуацією, тобто з реагуванням на інциденти з небезпечними речовинами та евакуацією. Обговорення виявило плутанину щодо того, які відомства або міністерства відповідають за визначення, встановлення пріоритетів та захист критично важливої інфраструктури.

Велися тривалі дискусії про оголошення воєнного стану і наслідки для початку масових заворушень, якщо стан буде схвалено.

Обговорення стосовно подій в ядерній енергетиці були зосереджені головним чином на визначенні причини зупинки та ідентифікації альтернативних джерел енергії.

Обговорили відповідальність з оцінки збитків, отриманих в результаті можливих атак. Існували суперечки про те, чи несуть збройні сили або інше відомство відповідальність за проведення боротьби з безпілотниками; вони не були вирішені. Було коротке обговорення стосовно звернення

до міжнародної спільноти за допомогою в разі стихійних лих, програм роботи з цивільними та програм підтримки цивільної влади з питань оборони (DSCA), а також надання підтримки діям цивільної адміністрації (SCA).

Ввідна 3.1.1: День 52: 26 лютого, 5:00

Оператор газотранспортної системи Сенти (ОГТСУ) спостерігає швидке падіння тиску на декількох газовимірювальних станціях: Гребеники (газопровід-інтерконнектор Сента-Вела) і Каушани (газопровід-інтерконнектор Вела-Сента). Фізичний потік газу через південну частину Сенти і Вели припинено, що призводить до скорочення постачання газу в окремі райони Одеської області, розташовані недалеко від кордону з Румунією.

Реагування на Ввідну 3.1.1

Державні газові компанії збільшать видобуток газу на морі. Крім того, будуть прийняті посилені заходи безпеки для захисту трубопроводів. Оператори також будуть переходити в режим економії енергії там, де це можливо. Як високопріоритетні будуть визначені ключові об'єкти виробництва та постачальники газу, тому інші будуть серйозно обмежені в постачанні або воно буде навіть зведене до нуля.

Ввідна 3.1.2: День 54: 28 лютого, 08:00

Великі вибухи на об'єктах з виробництва та зберігання аміаку ПАТ «Одеський припортовий завод». В результаті вибуху є значний викид аміаку та інших небезпечних хімічних речовин в атмосферу. Повідомляється про десятки постраждалих на заводі. Отруйна хмара аміаку рухається в бік Одеси та сусідніх міст.

Реагування на Ввідну 3.1.2

Комісія з техногенно-екологічної безпеки і надзвичайних ситуацій Одеської області оголосить про евакуацію населення з регіону, координуватиме евакуацію та усуватиме наслідки на місці вибухів (постраждали та руйнування). Для підтримки зусиль з евакуації будуть використовуватися регіональні засоби громадського транспорту. Поліція підтримуватиме порядок і здійснюватиме контроль за дорожнім рухом. Існує внутрішня нормативно-правова база для об'єктів критичної інфраструктури, що охоплює ці сховища. На регіональному рівні розроблений і буде реалізований план реагування стосовно об'єктів критичної інфраструктури.

Ввідна 3.1.3: День 54: 28 лютого, 17:00

Спостерігаються значні затримки з розвантаженням і завантаженням суден у портах Одеси, Чорноморська, Південного, Херсона. Було припинене постачання вже замовленого вугілля. Брак вугілля та інших видів палива призводить до скорочення вироблення тепла й електроенергії, а в деяких регіонах країни - до повного припинення вироблення електроенергії.

Реагування на Ввідну 3.1.3

Атомна електростанція в регіоні збільшить виробництво електроенергії. Крім того, гідро-електростанції також можуть збільшити виробництво і підтримати регіон. Фактичні поставки вугілля і палива не є критичними. Пріоритетна увага приділятиметься енергопостачанню об'єктів критично важливої інфраструктури. Некритичні об'єкти будуть перенаправляти енергію на критично важливі об'єкти. Регіон зможе вистояти в цій ситуації.

Ввідна 3.1.4: День 55: 1 березня, 11:00

Південно-Сентська атомна електростанція раптово вимушено переходить до аварійної зупинки. ЗМІ Бастана звинувачують постачальника ядерного палива з США, а «корумпована влада» Сенти повідомляє про те, що на атомній електростанції стався масштабний інцидент і є значний викид радіації.

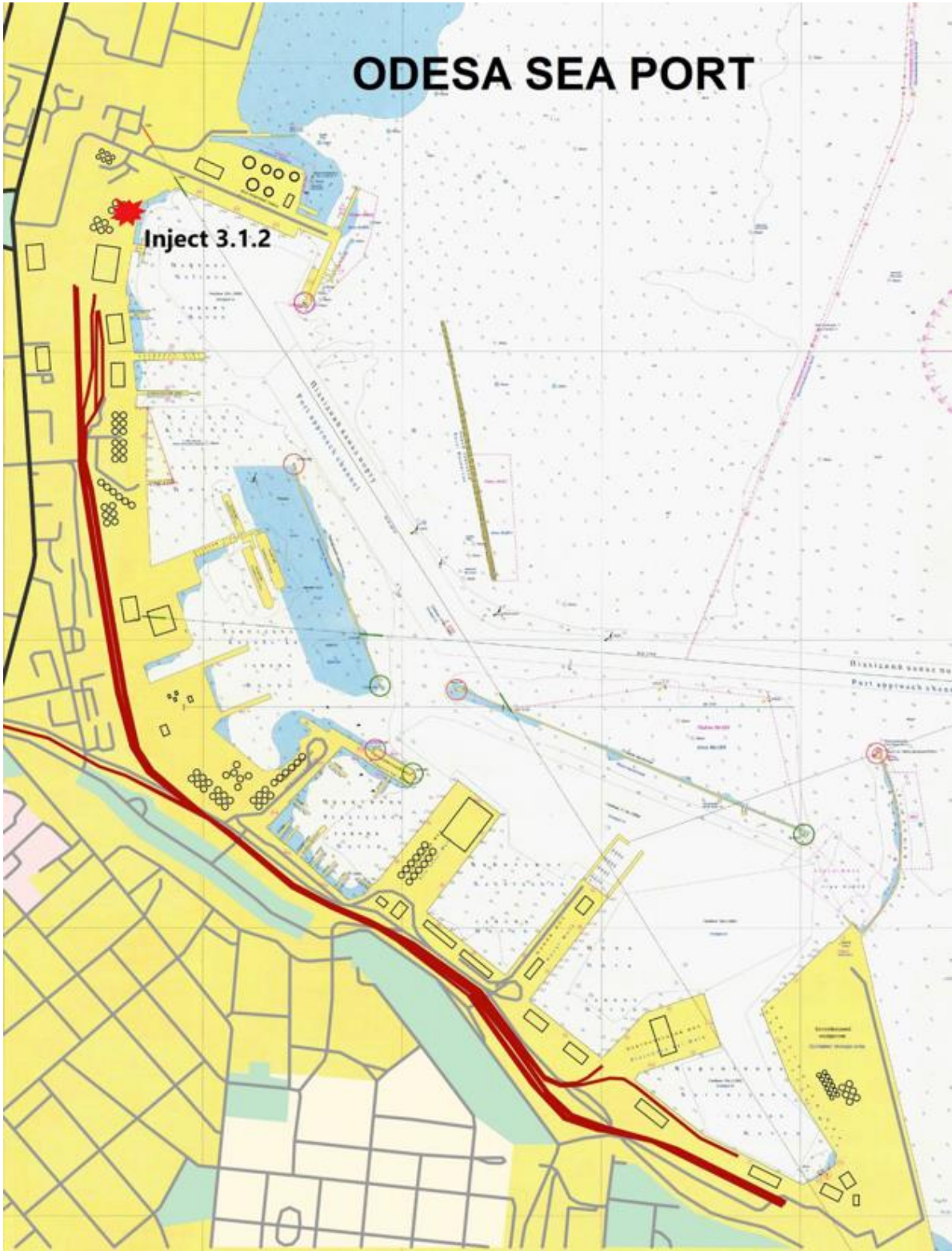
Реагування на Ввідну 3.1.4

Існують спроможності відновити роботу атомної електростанції в разі її зупинки. У цьому випадку схоже, що це була звичайна проблема технічного обслуговування, яку противник спробував використовувати у своїй кампанії з дезінформації. Місцеве населення буде проінформоване про фейкові новини та належне відновлення.

Ввідна 3.1.5: День 55: 1 березня, 12:30

Повідомляється, що Дністровська гідроакumuлююча електростанція зазнала нападу з використанням групи безпілотних літальних апаратів на малій висоті. Пошкоджено машинне відділення. Гідроелектростанція відімкнена від електромережі. Починається неконтрольований витік води з водосховища.





Реагування на Ввідну 3.1.5

По-перше, постраждалим буде надана медична допомога. Після початкового розслідування буде оголошена антитерористична операція. Про це буде негайно повідомлено Велу, оскільки, ймовірно, виникне небезпечна повінь і будуть потрібні заходи з евакуації. Необхідно буде провести оцінку того, чи також потребуватиме евакуації населення в місцевому регіоні.

Технічні фахівці на місці будуть вживати заходів щодо зниження наслідків, намагаючись звести збитки до мінімуму, наскільки це можливо. Державна служба з надзвичайних ситуацій направить на місце технічних фахівців, аби розпочати необхідний ремонт.

Цей інцидент вплине на всю країну, тому інші регіони впроваджуватимуть режим альтернативного розподілу електроенергії та перерозподілятимуть ресурси відповідно до встановлених пріоритетів і планів. Більш імовірно, що стосовно критичної інфраструктури, яка може стати ціллю атак, будуть прийняті посилені заходи безпеки, які включатимуть засоби боротьби з безпілотниками, й будуть розгорнуті сили. Щодо іншої критичної інфраструктури також підвищать заходи безпеки за рахунок посиленого патрулювання тощо.

3.4. Епізод 4: Гібридна війна

Напруженість у відносинах між Бастаном і Сентою досягла найвищого рівня за всю їх історію. Військова розвідка Сенти повідомила про безпрецедентне нарощування військових сил і засобів на базах Бастанського флоту в морі Нуар. На острові Тотара почала відбуватися значна кількість провокаційних нещасних випадків. Повідомлення про втрату сигналів GPS і GSM на острові. Підключення до Інтернету на острові зникло.

У той самий час Сента продовжує стикатися зі збільшенням кількості кібератак на урядові та місцеві установи та постачальників критично важливих послуг. ЗМІ Бастана і Сенти повідомляють в агресивній манері про нездатність центральної та місцевої влади Сенти надавати населенню критично важливі послуги. Більш того, вищі командири Збройних сил Сенти в Києві та посадові особи Військово-морських сил в Одесі та на острові Тотара отримали електронні листи з непідтверджених профілів з прямим попередженням «не виконувати накази політичного керівництва Сенти, інакше вони та їхні сім'ї будуть в небезпеці».

Соціальні мережі сповнені повідомлень і активних дискусій про можливе відділення південної частини Сенти. Ті ж новини поширюються через офіційні вебсторінки регіональних рад. Все вищевказане призводить до тиску та напруження всередині державних установ, правоохоронних органів і збройних сил. За останні 24 години різко посилилися вуличні демонстрації проти уряду Сенти, а саме в центральних містах південних регіонів: Одесі, Миколаєві та Херсоні. В результаті уряд функціонує на межі можливого, а населення збентежене.

На тлі значних кібератак, психологічного тиску, поширення дезінформації і дедалі більших вуличних протестів у південних регіонах на острові Тотара раптово висадилася значна кількість о/с збройних сил без розпізнавальних знаків. Доступ до порту острова Тотара заблокований вантажними суднами без розпізнавальних знаків і прапора держави. Доступ по воді до острова Тотара відрізаний. Бурові установки для видобутку вуглеводнів на острові Тотара, розташовані у ВЕЗ Сента, були захоплені й тепер знаходяться під повним контролем озброєних людей без розпізнавальних знаків.

Реагування на Епізод 4

Учасники погодилися з тим, що між Сентою і Бастаном існує стан війни і що буде оголошено воєнний стан. Було вирішено, що ВМС і морська піхота повинні розібратися з ситуацією на острові Тотара.

Були обговорені прохання про міжнародну підтримку. Учасники визнали, що територіальні вторгнення сил Бастану виправдовують міжнародну реакцію з боку НАТО, Ради Безпеки ООН та інших.

Учасники погодилися з тим, що для відновлення GSM потрібна співпраця уряду з представниками телекомунікаційної галузі. Не було чітко визначеного процесу координації співпраці між урядом і приватним сектором.

Ввідна 4.1.1: День 56: 2 березня, 05:00

Озброєні люди без розпізнавальних знаків захопили вісім газових вишок біля острова Тотара у ВЕЗ Сенти. Вони висадилися на вишки за допомогою вертольотів і захопили їх.

Реагування на Ввідну 4.1.1

Раніше в сценарії в цих місцях були розгорнуті додаткові засоби безпеки, в тому числі посилена присутність сил безпеки на морі, заходи безпеки підводних газопроводів, місць установки нафтових вишок, а острів був захищений додатковими військовими ресурсами.

Учасники оцінили, що така атака з вертольотів була б відбита, і будь-які захоплені бурові установки були б швидко відбиті, якби ці сили не отримали значної підтримки з боку Бастана.

Ввідна 4.1.2: День 58: 4 березня, 02:00

Вночі на острів Тотара десантується значна кількість добре озброєних людей без розпізнавальних знаків. Повідомлення про захоплення місцевих установ і основної військово-морської бази Сенти на острові. Для повного блокування доступу до військово-морської бази використовуються вантажні судна без розпізнавальних знаків і прапорів держави. Втрата сигналу GSM на острові та в Південному регіоні Сенти.



Реагування на Ввідну 4.1.2
Немає відповіді

3.5. Епізод 5: Посткризова стабілізація

Цей епізод присвячений посткризовому відновленню та процесу стабілізації. Посткризова стабілізація відбувається після закінчення кризового сценарію – з 7 березня 20XX року. Також потрібно обговорити питання управління в кризових ситуаціях.

Кожному синдикату буде запропоновано кілька питань для обговорення посткризової стабілізації.

Посткризова стабілізація

1. Яким ви бачите механізм вдосконалення системи захисту критичної інфраструктури на основі результатів управління в кризових ситуаціях?

Відповідь

Учасники запропонували таке: прийняти закони, які чітко визначають органи, обов'язки та відповідальність щодо захисту та підвищення стійкості критично важливої інфраструктури; встановити чітку вертикаль підпорядкування для оптимізації процесу прийняття рішень і забезпечення єдності зусиль на всіх рівнях управління; затвердити, здійснювати й оновлювати за потреби набір планів ЗКІ для усіх рівнів державного управління: національного, регіонального й місцевого; і розробка програм навчання і тренувань у сфері ЗКІ.

2. Чи бачите ви необхідність у вдосконаленні чинної нормативної бази щодо ЗКІ?

Відповідь

Учасники відзначили, що нині не існує нормативної бази – у кожного відомства є свої власні укази та постанови, але немає нічого, що об'єднувало б усіх їх. Було визначено кілька речей, які, на думку членів групи, можна було б зробити для поліпшення чинної нормативної бази, а саме: підвищення строгості покарань за атаки на об'єкти КІ; класифікація КІ на основі пріоритетності; і розробка закону (Національної концепції стійкості) для захисту критичної інфраструктури, в якому викласти обов'язки та відповідальність у сфері ЗКІ. Ще було визнано, що поточні плани, ймовірно, не узгоджуються з проектом закону про ЗКІ, тому необхідною буде додаткова робота для забезпечення узгодженого регулювання.

3. Чи необхідно створювати єдиний державний орган для координації захисту критичної інфраструктури (підпорядкований Президенту/РНБО/Кабінету Міністрів) або делегувати повноваження вже наявним державним органам?

Відповідь

Учасники погодилися з тим, що такий орган повинен бути створений, але також підкреслили, що тільки Кабінет Міністрів має повноваження на створення цього органу і він повинен підпорядковуватися Кабінету Міністрів.

4. Коли в останній раз оновлювалися/склалися заходи/плани, що забезпечують безперервність функції управління критичною інфраструктурою, на національному, регіональному та місцевому рівнях?

Відповідь

Учасники обговорили, що після прийняття законопроєкту можуть бути складені плани, які відповідатимуть цьому законопроєкту, які відповідним чином виконуватимуться. Однак практичні напрацювання існують в таких секторах, як енергетика, громадянське суспільство і боротьба з тероризмом. Поняття «критична інфраструктура» не включене в чинну нормативну базу. Хоча відпрацьовуються та здійснюються заходи, визначені в галузевих планах. Існує план об'єднання розрізнених в цей час нормативних баз в єдину структуру, що стосуватиметься критичної інфраструктури та її захисту. Нещодавно президентом була схвалена Концепція національної стійкості та нині здійснюється планування щодо розробки всебічної нормативної бази в галузі критичної інфраструктури та її захисту.

3.6. Ключові висновки

Потреба у створенні Національного координаційного агентства критичної інфраструктури (КІ).

Стійкість до гібридних загроз/атак вимагає ситуативної обізнаності на національному, регіональному та місцевому рівнях. В ході навчань була підкреслена необхідність створення Національного координаційного центру критичної інфраструктури для аналізу розвідданих та обміну інформацією з національними, регіональними та місцевими акторами, які приймають рішення. **Рекомендація:** Створити міжвідомчий Національний координаційний центр критичної інфраструктури з регулюванням на рівні Кабінету Міністрів для: аналізу загроз; надання вказівок і попереджень про

потенційні загрози та ризики всіх видів небезпеки як в стаціонарних умовах, так і у відповідь на кризи; і для сприяння обміну інформацією, пов'язаною з КІ, з органами влади на всіх рівнях державного управління та приватного сектора за потреби, оскільки в цей час відсутня нормативно-правова база. Ця урядова установа повинна мати повноваження надавати вказівки та керівні інструкції всім установам для затвердження Кабінетом Міністрів. Цей процес повинен бути законодавчо закріплений. Для виконання цієї ролі може бути трансформована Комісія з надзвичайних ситуацій та техногенної безпеки.

Потреба в стандартизованій методології оцінки вразливості критичної інфраструктури. Розробка та впровадження змістовних заходів захисту КІ та забезпечення стійкості залежить від визначення відносного ризику для критично важливих інфраструктурних систем та активів. У той час як оцінювання вразливості проводиться на секторальному рівні, є потреба в їх перегляді та оновленні в рамках централізованого процесу. В ході проведення навчань була підкреслена необхідність розробки та впровадження централізованої стандартизованої методології оцінки ризиків для КІ. **Рекомендація:** Розробити стандартизовану методологію оцінки ризиків для КІ, засновану на міжнародних стандартах оцінки ризиків (ISO 31000) або інших програмах оцінки, що зараз використовуються іншими країнами.

Потреба в національній таксономії та базі даних критичної інфраструктури. Реалізація планів, регламентів і процедур для захисту критично важливої інфраструктури та підвищення її стійкості вимагає чіткого розуміння секторів, систем і активів КІ. У ході проведення навчань була виявлена потреба у створенні Національного кадастру систем і активів КІ. Застосування детальної структурованої системи, що допомагає класифікувати активи за секторами, підсекторами, сегментами, підсегментами й типами активів, зводить до мінімуму ймовірність плутанини. **Рекомендація:** Розробити стандартизовану таксономію даних національної інфраструктури, яка встановлює детальну і структуровану термінологію, що полегшує пошук даних, управління ними та забезпечує обмін даними між органами влади на всіх рівнях державного управління.

Спроможності протидії безпілотним літальним апаратам. У зв'язку з чимраз вищою загрозою з боку безпілотників учасники визначили, що Україна має обмежені спроможності для ефективною протидії цим загрозам. В цей час у військових обмежені спроможності щодо знищення безпілотників, а Україні не вистачає сучасних технологій для найкращої протидії безпілотникам. Крім того, кільком відомствам, окрім військових, потрібні технічні знання і спроможності для знищення цих загроз. **Рекомендація:** Надати відповідним установам, відповідальним за захист критичної інфраструктури, технічний досвід і спроможності для відбиття таких атак. Розглянути шляхи отримання новітніх технологій та передового досвіду від міжнародних партнерів.

Система оцінки ризиків є реактивною (реагування на випадки), а не превентивною. Зараз стратегічне планування зосереджено на заходах реагування на випадки. Відсутня система попереджувального (проактивного) стратегічного планування, яка оцінює ризики та фокусується на запобіганні. Немає ані організації, відповідальної за це, ані персоналу, здатного виконувати ці обов'язки. **Рекомендація:** Створити організацію, яка нестиме відповідальність і буде здатною проводити стратегічні оцінки ризиків. Цю відповідальність повинен взяти на себе міжвідомчий національний координаційний центр критичної інфраструктури, який буде створений.

4. Синдикат (Група) 2: Кібербезпека



Синдикат «Кібербезпека» обговорює заходи реагування на ввідні в рамках епізоду під час КШН «НАТО CORE 20 – Чорне море».

4.1. Епізод 1: Доконфліктна фаза: Гібридний вплив

Посилюється політичне та економічне залякування з боку влади Бастану. На підставі угоди про транзит газу, яка була підписана між Бастаном і Сентою минулого року, уряд Бастану звинуватив Сенту в порушенні положень угоди. Сента заперечує будь-які порушення. Однак ЗМІ Бастану і деякі ЗМІ Сенти, контрольовані Бастаном, продовжують поширювати повідомлення про порушення Сенти, підкреслюючи важливість відповідної угоди для енергетичної безпеки Європи, оскільки транзит газу в європейські країни частково забезпечується через територію Сенти.

Ситуацію ускладнює той факт, що між Бастаном і Велою не укладено новий контракт на постачання газу. Враховуючи суперечки щодо договірних положень, Бастан тимчасово істотно скорочує постачання газу в Велу. Вела максимально відбирає газ з транзитного трубопроводу, обмежуючи постачання газу споживачам Сенти в Одеській області, недалеко від кордону з Румунією.

Тим часом Бастан ввів обмеження на імпорт товарів сільського господарства, обробної промисловості та металевих виробів, палива, хімікатів і нафтопродуктів із Сенти. Крім того, Бастан припиняє постачати нафтопродукти в Сенту автомобільним, залізничним транспортом і трубопроводами.

В Інтернеті були виявлені три вебсайти з ідентичним візуальним оформленням і функціями офіційних вебсайтів Оператора ГТС Сенти, Оператора PSG і компанії «Нафтогаз». Крім того, на

електронні адреси регіональних урядових установ Сенти були надіслані листи з фішинговими функціями та прикріплені текстові документи Microsoft Word.

У ЗМІ з'явилися повідомлення про потужну кібератаку на внутрішню мережу Liebherr в Німеччині. В результаті портові крани в морському порту Поті в Зестані перестали працювати.

З середини грудня берегова охорона Сенти регулярно повідомляє про присутність Військово-морських сил Бастана у ВЕЗ Сенти. Повідомляється, що Бастан проводив військові навчання в морі Нуар у безпосередній близькості від фарватерного проходу торгових і пасажирських суден з/в порти Одеської області.

Реагування на Епізод 1

Учасники реагували на ситуацію, що загострювалася, за всіма трьома ввідними в першому Епізоді з високим ступенем технічної деталізації та значною кількістю дискусій, що стосувалися координації на високому рівні та необхідних дій від державних і приватних компаній. Члени Синдикату не були дуже стурбовані початковими DoS-атаками на загальнодоступні вебсайти центральних урядових установ Сенти, а обговорення фокусувалося на тому, які вебсайти перебували під захистом служби кібербезпеки та коли різні рівні державного реагування (наприклад, команда реагування на комп'ютерні надзвичайні події України (CERT-UA) або Служба безпеки України (СБУ)) повинні бути поінформовані та залучені до реагування.

Ввідна 1.2.1: День 11: 16 січня, 12:00

Загальнодоступні вебсайти центральних урядових установ Сенти (Парламенту, Адміністрації Президента, Міністерства оборони та Міністерства закордонних справ) та регіональних державних адміністрацій недоступні. Експерти підозрюють DoS-атаку (відмова в обслуговуванні) на ці ресурси.

Реагування на Ввідну 1.2.1

Акторами реагування на цю ситуацію будуть Служба безпеки (СБУ), Державна служба спеціального зв'язку та захисту інформації для кожної організації, що зазнала атаки (стандартні процедури протягом двох годин). Також повинні бути залучені підрозділи, відповідальні за інформаційну безпеку всіх зацікавлених сторін, що зазнали нападу. Ніяких істотних впливів і каскадних ефектів виявлено не було. Якщо це частина великої операції, то потрібна подальша координація між владними структурами, але очікувана нескладна DOS-атака не матиме значного впливу. негайним необхідним реагуванням буде інформування CERT-UA та активація резервних копій вебсайтів (оскільки всі вони дублюються з точки зору апаратного забезпечення, з кількома інтернет-провайдерами та IP-адресами (в тому числі закордонні сервери для забезпечення резервування та доступності)). Крім того, буде введено в дію комунікаційний план для забезпечення доступу населення до точної інформації від центральної влади та обласних державних адміністрацій. Основні проблемні питання носили не технічний або процедурний характер, а скоріше були пов'язані з оповіщенням і поширенням точної інформації серед широких верств населення. Було досягнуто взаємної згоди в тому, що в подібному конкретному випадку DOS-атаки населення могло б дізнатися, що відбувається, зайшовши спочатку на сайт Президента, а потім на сайт обласної державної адміністрації. Для цих випадків Уряд запровадив план дій у нештатних ситуаціях, тому в них є альтернативні джерела інформації з перевірених облікових записів у Telegram і Facebook.

Коментарі до обговорення: Початкова розмова велася навколо інформування національного командного органу та Національного центру кіберкомандування. Група визначила кілька важливих вимог до термінів інформування зацікавлених сторін (7 днів для максимального часу направлення

повідомлень про атаку в письмовій формі та вимога до Інтернет-провайдера впродовж одного дня провести заходи з управління та захисту від DoS-атак). Команда зосередилася на оцінці того, наскільки критичним є сервіс або вебсайт (який зазнав DoS-атаки) і які наслідки може мати його компрометація. Вони підкреслили, що з цієї DoS-атакою легше впоратися, ніж з більш комплексними атаками.

Ввідна 1.2.2: День 14: 19 січня, 02:00

Ймовірна кібератака поширюється на інші сектори – блокується доступ до сайтів важливих банківських систем (ПриватБанк, Ощадбанк), інформаційних агентств і порталів.

Реагування на Ввідну 1.2.2

Кожен банк окремо і Національний банк України координуватимуть дії з реагування зі сторони банків. Приватні інформаційні агентства матимуть свої власні внутрішні групи з кібербезпеки та реагування на кіберзагрози, а також звертатимуться до Національної поліції щодо порушення кримінальних проваджень. Цілком ймовірно, що через скоординовану атаку залучена буде також і Служба безпеки України (СБУ) як слідчий орган і орган реагування. Було обговорено вплив на вебсайти на протипагу впливу на банківську систему (наприклад, застосунки та транзакції), що суттєво вплинуло на оцінку наслідків. Якщо банківська система не зазнає впливу, то масової паніки не буде – або це буде індикатором майбутніх очікуваних подій. Можлива паніка виникне, якщо ці банки не зможуть виплачувати пенсії та використовуватися для оплати послуг. Чимраз більші побоювання з приводу можливості більш масштабних атак і втрати ключової інформації про події можуть викликати загальну плутанину і мати вплив на економіку і громадянське суспільство в цілому. Перелік деяких проблемних питань, які можуть перешкоджати ефективному реагуванню: систематика інцидентів та вимоги до звітності були визначені як проблема, оскільки немає визначення кіберкризи, а кожна державна та приватна установа має свої власні процедури та правила. Учасники відзначили низький рівень довіри до правоохоронних органів у приватних компаній, що призводить до організації роботи з охоронцями за контрактом або безпосереднього звернення в агентство спеціального зв'язку. Оскільки не було учасників з-поза меж великих державних компаній (наприклад, Національного банку України та «Нафтогазу»), то неможливо було отримати точку зору приватної компанії на події. Також було зазначено, що в той час, як Національний банк України координує дії/комунікацію щодо випадку з банківською системою, кожен банк також може здійснювати своє власне реагування, особливо в соціальних мережах.

Коментарі до обговорення: Ці зростаючі атаки стосуються приватних і державних організацій з різним рівнем ресурсів, захисту та вимог до реагування, і тому в Синдикаті було багато дискусій про відповідальних осіб і їх необхідні дії. Окрім звернення до Національної поліції щодо порушення кримінального провадження або звернення до приватної (за контрактом) служби безпеки, більшість компаній, таких як інформаційні агентства, не мають стандартних форм реагування або вимог до звітності, які можуть знадобитися для ефективного реагування з боку державних установ.

Члени Синдикату також обговорили необхідність створення більш надійних центрів реагування на кібератаки та укомплектування персоналом команди реагування на комп'ютерні надзвичайні ситуації України (CERT-UA) та Національної поліції. У той час як теоретично оператори та диспетчери доступні 24/7 для збору та обробки інформації, технічних деталей атак і для реагування на загрози

в співпраці з CERT-UA, реальність така, що у них немає можливостей. Це також створює проблеми при спробі визначити, чи пов'язані або скоординовані попередні та поточні інциденти, а також визначити, чи вони системні.

Ввідна 1.2.3: День 16: 21 січня, 11:00

Повідомлялося про атаки на сервісні центри виставлення рахунків онлайн та оплати комунальних послуг в Одеській області. Регіональний підрозділ кіберполіції реєструє скарги окремих громадян на те, що їх дані про спожиті комунальні послуги не відповідають точній інформації та, як наслідок, в системі є непогашені борги.

Реагування на Ввідну 1.2.3

Як органи реагування синдикат визначив приватну білінгову компанію у сфері комунальних послуг та команду реагування на комп'ютерні надзвичайні ситуації України (CERT-UA). CERT-UA - це не приватна компанія, а сервісні центри, які входять до складу комунального концерну, наприклад, Центр комунального сервісу в Києві. Група обговорила характер атаки - якщо вона буде спрямована на білінгову систему (а не на систему реєстрації та обліку), то наслідки будуть зведені до мінімуму. Були виявлені можливі каскадні ефекти (наслідки), зокрема, протестувальники на вулицях через виявлені борги. Необхідним реагуванням у цьому випадку було б змусити приватну білінгову компанію співпрацювати з Національною поліцією для початкового розслідування заяв про шахрайські рахунки. Це було розцінено як безперервна атака на стабільність в країні, тому координація буде здійснюватися між Офісом Президента та місцевою владою. Крім того, буде налагоджено зв'язок між підрозділами кібербезпеки, керівництвом компанії та засобами масової інформації в цілому з можливою координацією проведення пресконференцій та надання інших стратегічних повідомлень. Основним проблемним питанням було те, що приватна компанія повинна була б швидко і точно повідомити уряду технічну інформацію про інцидент. Приватні компанії неохоче підключаються до системи в разі кіберінцидентів, і не було виявлено жодної контактної особи. Крім того, очікувалися прогалини у можливостях кіберполіції діяти в подібній ситуації, оскільки наявна система була б переважана великомасштабними подіями та надмірними повідомленнями від громадян про проблеми з виставленням рахунків.

Коментарі до обговорення: Атаки на платіжні системи та системи обробки даних Пенсійного фонду як показує досвід призводили до затримок і сприяли дестабілізації в країні, однак враховуючи спосіб виставлення рахунків за газ існує кілька варіантів швидкого реагування (наприклад, користувачі платять свої прогнозовані суми, а не виставлені в рахунку суми). Одна з речей, яка допоможе заспокоїти людей і стабілізувати цю ситуацію, полягає в тому, що існує готова резервна копія, яка є аналоговою і незалежною від білінгової системи. Учасники відзначили, що пресрелізи вже надавалися, коли одного разу відбувалася така ситуація з пенсійними фондами, а форми реагування, ймовірно, будуть змодельовані на основі цього успішного прецеденту. Члени Синдикату також підкреслили, що після оголошення надзвичайного стану Державна служба з надзвичайних ситуацій може взяти на себе більшу частину необхідної координації та реагування, але спочатку буде потрібний план, схвалений Кабінетом Міністрів, аби визначити, наскільки критична ситуація.

Резюме учасників щодо Епізоду 1:

Епізод 1 розпочався як проста атака типу «відмова в обслуговуванні» (DoS) на урядові вебсайти та переріс в атаки на вебсайти банківських систем, новинні агентства і системи виставлення й оплати рахунків комунальних служб. Учасники відзначили, що в кожному випадку походження атак, їх координація і серйозність були невизначеними. Ввідні були складним завданням, оскільки вони

стосувалися як приватних, так і державних організацій з абсолютно різними рівнями ресурсів, захисту та вимог до реагування. Це створило два набори проблем, які необхідно було вирішити членам Синдикату: відповідальність за дії та звітність і координація реагування.

Державні організації повинні мати ресурси та персонал для реагування на події та мають тісну взаємодію зі службою безпеки та групами кризового реагування на національному та місцевому рівнях. Наприклад, Національний банк України належить державі та знаходиться під її регулюванням і контролем, інші банки перебувають у державній власності та під захистом міжнародної системи банківської безпеки. Якщо банківські системи недоступні протягом більш тривалого часу, ніж визначено, то про це інформують Національний банк України, а також є державне/національне реагування. На рівні кожного банку є ризик-менеджер, який відповідає за всі ризики, в тому числі кібер ризики. Банки зобов'язані звертатися до CERT-UA в певні терміни в залежності від серйозності атаки та її наслідків.

У приватному секторі система реагування складніша, адже окрім звернення до Національної поліції щодо порушення кримінального провадження або звернення в приватну (за контрактом) службу безпеки, більшість компаній, таких як інформаційні агентства, не мають стандартних форм реагування або вимог до звітності. Це підкреслило необхідність чіткіших визначень стосовно подій, що підлягають звітності, відносин між державним і приватним секторами й обміну повідомленнями. Було досягнуто взаємної згоди в тому, що у випадку збоїв у роботі інформаційних агентств або білінгових компаній населення могло б дізнатися, що відбувається, зайшовши спочатку на сайт Президента, а потім на сайт обласної державної адміністрації. Для цих випадків Уряд запровадив план дій у нештатних ситуаціях, тому в них є альтернативні джерела інформації з перевірених облікових записів у Telegram і Facebook, але вони можуть бути не в змозі збирати початкові звіти від компаній без вищого ступеня довіри та чіткіше встановлених вимог до звітності. Було відзначено, що немає визначення «критичної» ситуації, а є тільки набір загальних категорій. Це ускладнювало загальне урядове реагування на розподілений набір атак, особливо у сфері обміну повідомленнями та створення сенсацій на ранніх стадіях проблеми.

4.2. Епізод 2: Гібридні операції низької інтенсивності

На початку лютого погодні умови в південних районах Сенти погіршилися. Швидкість вітру досягає 50 м/с, що завдає значної шкоди, зокрема, в Одеській області.

Введені Бастаном обмеження на імпорт товарів сільського господарства, обробної промисловості та металевих виробів, палива, хімікатів і нафтопродуктів із Сенти сприяють занепаду економіки Сенти, яка вже знаходиться в стані рецесії. Пробастанські активісти використовують економічний спад як шанс посилити протести проти уряду Сенти. Соціальна напруженість досягла свого піка, коли в Інтернеті поширилася новина про рішення Одеської міської ради про вихід Одеської області зі складу Сенти.

Діяльність пробастанських активістів та інциденти у сфері кібербезпеки постійно порушують роботу Одеського морського порту. Крім того, цивільні судна і кораблі берегової охорони Сенти повідомляли про технічні неполадки у роботі своїх навігаційних систем.

Крім того, судна Бастана діють агресивно проти риболовецьких суден Сенти. Кораблі берегової охорони Бастана залякують і погрожують вантажним суднам Сенти, а також суднам іноземних держав. Нещодавно Військово-морські сили Бастана надали підтримку незаконній діяльності з

розвідки газу і встановлення бурових установок на території ВЕЗ Сенти. Навколо бурових установок був встановлений цілодобовий охоронний патруль Військово-морських сил Бастану.

Реагування на Епізод 2

Учасники реагували на ескалацію атак на численні державні та приватні системи протягом всього Епізоду 2, починаючи зі спотворення вебсайту, потім ситуація ускладнилася запуском шкідливого коду в мережі Банку «Південний» і пов'язаними з цим DDoS-атаками на Національний банк Сенти. Члени Синдикату звернули увагу на проблеми, пов'язані зі складними розмежуваннями повноважень і юрисдикції, коли приватний сектор піддається можливій атаці або зазнає збитків. Деякі моменти обговорення учасників були зосереджені на проблемі розуміння того, що відбувається і здатності розрізняти сигнал (фактичні кібератаки та гібридні війни) і шум (фактори навколишнього середовища і природні явища), що впливають на відповідні інформаційні системи. Учасники продемонстрували чітке розуміння спроможностей держави (наприклад, СБУ і Національного банку), але були більш невпевнені в спроможностях приватних компаній, рівнях готовності та специфічних для кібербезпеки вимогах, що пред'являються до приватного сектора. Обговорення також висвітлює проблеми, які все це створює для скоординованого реагування між державними та приватними структурами, а також для міжнародної спільноти. Численні учасники також навели відповідні історичні приклади та особистий досвід при розв'язанні таких проблем, як викриття інформаційних операцій, подібних описаній у цій ввідній.

Ввідна 2.2.1: День 24: 29 січня, 12:00

На сайті Одеської міської ради йдеться про те, що обласна влада вирішила проголосити незалежність від Сенти та стати Одеською Автономною Республікою.

Реагування на Ввідну 2.2.1

Необхідні органи реагування в цьому випадку - Служба безпеки України (СБУ), Офіс Президента, Парламент і Рада національної безпеки та оборони України. У цьому сценарії є потенціал для серйозних каскадних ефектів (наслідків), оскільки зміни на вебсайті можуть послужити міжнародною провокацією, а цей акт може стати першим кроком в активізації сепаратистських груп і може привести до державного перевороту. Необхідним реагуванням було б інформування Збройних сил (якщо це реальна інформація), Державної служби спеціального зв'язку та захисту інформації та CERT-UA - все це було б зроблено негайно. Центральний уряд зосередився б на спростуванні цієї інформації, роблячи заяви та надаючи роз'яснення, що це була злочинна дія. Поінформовані були б й інші гілки влади, а інформація про характер нападу була б широко розповсюджена. Крім того, буде введено в дію комунікаційний план для забезпечення доступу населення до точної інформації від центральної влади та обласних державних адміністрацій. Існує стурбованість щодо термінів, пов'язаних з певними частинами реагування, і команда визнала вкрай важливим переконатися, що вебсайт не був відключений навмисно, оскільки це може бути показником правдивості тверджень. Правильне спростування і контроль над повідомленням і пов'язаними з ним часовими рамками визначили б різницю між тим, чи є повідомлення вірусним і таким, що дестабілізує, або ж воно має лише невеликий вплив. Розмежування повноважень і юрисдикції в цій ситуації є складним, оскільки СБУ є тим органом, який вирішує/визначає, що є правдою, і якщо це кіберзлочин, то за справу береться кіберполіція. СБУ буде обробляти інформацію і повідомляти про неї уряд і Президента, вони є основним майданчиком для отримання цієї інформації від Національної поліції, до якої громадяни будуть звертатися в першу чергу.

Коментарі до обговорення: Обговорення учасників було зосереджено на визначенні реальної ситуації після того, як було здійснене початкове реагування. Від експлуатаційних команд вебсайтів

вимагалось б з'ясувати, що і як сталося, а потім передати цю інформацію в СБУ і Національну поліцію, а також в обласну адміністрацію, оскільки вони знаходяться в підпорядкуванні. Характер події (чи то простий злочин або спроба державного перевороту з боку суб'єкта-держави) визначатиме подальші дії. Члени Синдикату також обговорили терміни визначення правди про подію та передового досвіду для надійної комунікації з населенням. Як відправна точка для викриття інформаційних операцій, подібних до тієї, що описана в цій ввідній, були використані історичні події в Севастополі.

Ввідна 2.2.2: День 30: 4 лютого, 16:00

Кібератака на сайт Одеського морського порту. Адміністратори втрачають контроль над поштовим сервером. Вебсторінка, що вказує місце розташування вантажних суден у межах портових терміналів, недоступна. Після відновлення вебсайту більша частина інформації про обсяг і статус вантажу зникла.

Реагування на Ввідну 2.2.2

Необхідними органами реагування на цей сценарій були б морський порт, який є власником вебсайту, який несе відповідальність за дані. Національна поліція також провела б розслідування інциденту і могла б повідомити про нього Службу безпеки (СБУ). Наслідки цього сценарію полягають в тому, що під загрозою перебуває робота порту і це впливає на розклад руху суден, навантаження, розвантаження і виставлення рахунків. Можливі каскадні наслідки – міжнародні проблеми, судовласники, вантажовласники – всі вони причетні до цієї події, в тому числі міжнародні наслідки та звернення до страхових компаній. Необхідне реагування полягало б у тому, що морський порт та його приватна служба безпеки та команда, що відповідає за базу даних, відповідали б за відновлення резервних копій даних, інформування громадськості про інцидент та відновлення нормальної роботи порту. СБУ розслідувало б характер атаки та співпрацювало б з Національною поліцією, аби визначити походження атаки та вжити відповідних заходів державного реагування. Деякі проблемні питання, які відзначила група: відсутність довіри між морським портом та іншими приватними підприємствами ускладнює скоординоване реагування. Учасники підкреслили значну шкоду репутації та проблеми співпраці, які викликав обмін даними з Національною поліцією. Нині немає вимог до звітності та офіційних позначень критичної інфраструктури.

Коментарі до обговорення: Члени Синдикату погодилися з тим, що Служба безпеки України (СБУ) має регіональне управління з підрозділами захисту національних інтересів у портах і що вони відіграватимуть важливу роль у реагуванні. CERT-UA в Києві буде тим органом, який дасть вказівки щодо того, як діяти в кіберпросторі (якщо їх про це повідомлять порт і СБУ). Резервні копії потрібні для всіх баз даних, оскільки це критично важлива інфраструктура (вона вже існує). Міністерство інфраструктури має визначити необхідні дії та забезпечити дотримання цього правила (яке, на думку членів синдикату, не дотримувалося суворо). Необхідно посилити державний контроль за розміщенням електронних ресурсів на об'єктах критичної інфраструктури, що перебувають у приватній власності.

Ввідна 2.2.3: День 40: 14 лютого, 20:00

У засобах масової інформації та в соціальних мережах наявна інформація про загальнодоступність інформації про виставлення рахунків за комунальні послуги із зазначенням особистих даних клієнтів, таких як ім'я, адреса, номер телефону, адреса електронної пошти.

Реагування на Ввідну 2.2.3

Для захисту та перевірки інформації необхідним органом реагування стає білінгова компанія, а що стосується кримінального розслідування і державного реагування, то місцева і Національна поліція

будуть необхідними органами реагування. Оприлюднення цієї інформації призведе до масової плутанини та скарг. Якщо це правдиві дані, то це може призвести до масового шахрайства щодо українців. Якщо персональні дані включають дані громадян ЄС, то вступає в силу національне законодавство та існує ймовірність штрафів за порушення положень Загального регламенту ЄС про захист персональних даних. Повинно бути проведене розслідування Національної поліції, аби визначити справжність і джерело витоків інформації. Постачальник послуг (дочірня компанія більшої державної організації, яка управляє постачанням газу) буде нести відповідальність за будь-які негативні наслідки для громадян України та іноземних громадян. Залежно від засобів поширення інформації, що дозволяє встановити особу (персональні дані), може знадобитися залучення структур на вищому національному рівні. Будуть залучені CERT-UA і Рада національної безпеки і оборони. Проблемним питанням, яке відзначила група, була відсутність спеціальної команди з видалення кримінального контенту в Інтернеті для подібних випадків (нині такими питаннями займаються органи внутрішніх справ). Члени Синдикату з Міністерства оборони висловили стурбованість з приводу того, що влада усуне джерело персональних даних, але в цілому реагування групи полягало в тому, що немає ніякого механізму щодо витоків в месенджерах соціальних мереж. Використання програмних рішень (автоматизований моніторинг) і страхування від кібер ризиків повинні бути обов'язковими для забезпечення зниження ризиків, але зараз цього немає. Міжнародні стандарти для визначення рівня кібернетичної готовності та планів реагування на кібератаки також допомогли б ефективно реагувати.

Коментарі до обговорення: Члени Синдикату не хотіли робити поспішних висновків і пов'язувати цю подію з іншою частиною Епізоду, оскільки неясно, чи дійсно це справжні дані та чи цей витік даних не був зроблений незадоволеним співробітником, або в рамках якихось більших операцій. Спроможності уряду та/або стратегічні партнерські відносини з власниками соціальних мереж щодо варіантів обмеження або відмови в доступі до персональних даних в Інтернеті були частиною поглибленого обговорення учасниками, але не призвели до будь-яких висновків.

Відна 2.2.4: День 43: 17 лютого, 10:00

Танкер, що належить Сенті, раптово втрачає управління і стикається з вантажним судном Бастана у ВЕЗ Сенти, що призводить до значного розливу нафти. Бастан звинувачує Сенту в диверсії.

Реагування на Ввідну 2.2.4

Необхідними органами реагування у цій ситуації були б Морська Адміністрація (торгове управління, а не військово-морські сили) у співпраці з національними міністерствами та Генеральним штабом Збройних Сил України, СБУ та міжнародними партнерами. Ця подія може мати серйозні економічні та міжнародні наслідки. Реагування вимагало б координації розслідування і обміну повідомленнями на національному рівні (Рада національної безпеки і оборони України, СБУ, Національна поліція, Генеральний штаб Збройних Сил України, розвідка, Міністерство внутрішніх справ і Міністерство цифрової трансформації). Збір доказів і записи повинні бути отримані Державною службою спеціального зв'язку та захисту інформації. Національний координаційний центр кібербезпеки може звернутися для того, аби відстежити сигнали, які створювали завади, або зібрати докази. Проблемним питанням є те, що немає протоколу для того, що необхідно робити, але реагування на подібну подію буде продиктовано ширшими геополітичними вимогами та координуватиметься на національному рівні.

Коментарі до обговорення: Члени Синдикату не були впевнені, чи була у цієї події кібер-складова. Вони представили ідеї про те, які так чи інакше підтвердити, що потрібна подальша участь кібер-синдикату.

Ввідна 2.2.5: День 46: 20 лютого, 10:00

У мережі банку «Південний» виявлено шкідливий код. На ІТС Державного офісу Національного банку «Сента» в Одеській області здійснена DDoS-атака.



Реагування на Ввідну 2.2.5

Перше реагування в цій ситуації було б від місцевого банку (банк «Південний» зареєстрований в Одеській області). Національний банк України регулює кібербезпеку всієї банківської системи. Ця подія може мати серйозні економічні та міжнародні наслідки, в тому числі масова паніка і втрата довіри до банківської системи з боку українського народу. Очікуване реагування полягатиме в тому, що банк розпочне процедури управління інцидентами, а комерційний банк проінформує Національний банк про інцидент. Існує спеціальна платформа (об'єднує понад 60 банків) для обміну інформацією про реагування на інциденти (заповнення спеціальних форм). НБУ надає рекомендації щодо форм реагування, а інформація передається CERT-UA для подальшої експертно-криміналістичної експертизи. Учасники відзначили, що стандартних форм реагування на таку проблему не існує - є вимоги, але немає чітких інструкцій і процедур для такої ситуації. Сайт буде досліджено, а за необхідності будуть залучені міжнародні експерти. Необхідно оцінити масштаби ситуації, аби визначити, чи є це актом війни.

Коментарі для обговорення: Члени Синдикату вказали, що банк належить до категорії критичної інфраструктури, тому будь-які інциденти повинні відповідати вимогам управління в критичних ситуаціях. Представники НБУ впевнені, що DDoS-атака не буде ефективною (і у них є спеціальні сервіси, які вони купили, аби допомогти їм впоратися з цим).

Резюме учасників щодо Епізоду 2:

Зростаюча серйозність кібератак в Епізоді 2 підкреслила різницю між державними та приватними організаціями з точки зору їх спроможностей, координації та реагування на кібератаки. Члени Синдикату погодилися з тим, що Служба безпеки України (СБУ) має регіональне управління з підрозділами захисту національних інтересів у багатьох найважливіших галузях національної промисловості (в тому числі порти) і що вони відіграватимуть важливу роль у більшості реагувань.

Для комерційної банківської системи процедури управління інцидентами були чітко встановлені та, як правило, передбачали інформування комерційним банком НБУ про описаний інцидент. Існує спеціальна платформа (об'єднує понад 60 банків) для обміну інформацією про реагування на інциденти (заповнення спеціальних форм). НБУ надає рекомендації щодо форм реагування, а інформація передається CERT-UA для подальшої експертно-криміналістичної експертизи.

Для приватного сектора було два ключових висновки. По-перше, відсутність довіри між приватним сектором і правоохоронними органами ускладнює скоординоване реагування. Учасники підкреслили значну шкоду репутації та проблеми співпраці, які викликав обмін даними з Національною поліцією. По-друге, зараз немає вимог до звітності та офіційних позначень критичної інфраструктури. Наприклад, у випадку атаки на базу даних порту для всіх баз даних потрібні резервні копії, однак члени Синдикату не вірили, що ця вимога суворо дотримується.

4.3. Епізод 3: Фаза конфлікту: Гібридні операції високої інтенсивності

Критична інфраструктура Сенти піддається широкому спектру ударів кінетичною і некінетичною зброєю. Перебої в роботі газопроводу з транспортування природного газу в Південному газотранспортному коридорі позначаються на постачаннях газу в Південний регіон Сенти та сусідні іноземні держави. Додатково існує загроза зриву опалювального сезону не лише в південній частині Сенти, але й у Харківській і Луганській областях, які, зокрема, сильно залежать від постачання газу з Бастана.

На півдні Сенти на третину збільшилася кількість надзвичайних ситуацій, пожеж і нещасних випадків, викликаних підпалами й терористичними актами з використанням вибухових речовин, що, своєю чергою, призвело до значного збільшення числа постраждалих. Є підозра про значний інцидент на ПАТ «Одеський припортовий завод», де повідомляється про значний викид небезпечних хімічних речовин.

Поширюється інформація про зриви в роботі Південно-Сентської АЕС. ЗМІ Бастана звинувачують владу Сенти у викидах радіації. Майже одночасно поширюється інформація про атаку на гідроакумуляуючу електростанцію.

Масовані кібератаки порушують роботу Одеського морського порту, в тому числі транспортування й обробку вантажів. Нападу зазнали банківські системи відділень Ощадбанку і ПриватБанку в Одеській області.

Через місяць після першої кібератаки на внутрішню мережу Liebherr в Німеччині сталася серія незначних кібератак на портові крани Liebherr по всій Європі.

У морській сфері кораблі ВМС Бастана збільшують свою присутність у ВЕЗ Сенти, використовуючи Військово-морські навчання, припиняючи міжнародні морські перевезення пасажирів і вантажів.

Реагування на Епізод 3

Члени Синдикату вели жваву дискусію навколо введення складніших проблем, таких як кібератаки вищого рівня, несправні сигнали від обладнання і, нарешті, великомасштабні масові жертви в результаті гібридних кібер-операцій. Вони також підкреслили той факт, що на об'єктах завжди знаходяться кіберкоманди та групи моніторингу, які стежать за роботою цього дуже дорогого обладнання, але вони, швидше за все, будуть розглядати ці проблеми з технічної точки зору, а не їх кібернетичний аспект. Ця невизначеність і тривалість часу, необхідного для належної перевірки кібератаки, залишалися центральними питаннями обговорення.

Учасники також покладалися значною мірою на СБУ як на центральний координаційний центр обміну інформацією та реагування на кіберзагрози, хоча це може бути відповідальністю як Державної служби спеціального зв'язку та захисту інформації, так і кіберполіції. Учасники вказали на сильний перекис у бік ролі СБУ, який сформувався через слабке дотримання закону. Вони також заявили, що СБУ самостійно проводить розслідування і вирішує, кого інформувати про такі різні події, і що, ймовірно, будуть посилені заходи захисту через збільшений рівень загрози. Такий підхід вносить дисбаланс у повноваження Державної служби спеціального зв'язку та захисту інформації та кіберполіції. Навчання, що проводяться СБУ, можуть включати або не включати кібертестування.

Ввідна 3.2.1: День 52: 26 лютого, 12:00

Раптово виходять з ладу автоматизовані системи документообігу операторів одеських портів. Втрачена вся інформація про зберігання та обробку вантажів у портах. Повідомляється про аналогічні інциденти в енергетичному та банківському секторах - послуги онлайн-банкінгу недоступні.

Реагування на Ввідну 3.2.1

У цьому випадку органами реагування повинні бути Національний координаційний центр кібербезпеки (НКЦК) і СБУ, які в координації з НБУ і місцевими відомствами будуть першими органами реагування. НБУ визначить, чи існує криза, і може вжити надзвичайних заходів у банківській системі. Заходи реагування на національному рівні координуватимуться, за потреби, Міністром внутрішніх справ. Всі три сфери мають вирішальне значення. Всі три сфери, що до яких здійснено атаку, взаємопов'язані. Відключення електроенергії, ймовірно, будуть першими та найбільш очевидними наслідками, за якими піде економічний збиток. Відключення електроенергії будуть домінувати над проблемою через каскадні ефекти (наслідки), що призведуть до відключення всього (наприклад, води, транспорту тощо). Інші каскадні ефекти можуть мати міжнародний рівень і стосуватися вантажів. СБУ, швидше за все, керуватиме у цій ситуації, оскільки вона відповідає за контртерористичні операції. СБУ проінформує НКЦК. НКЦК визначатиме штатне наповнення в команді та координуватиме реагування кіберцентру стосовно кожної сфери. Крім того, кожна організація звітує перед CERT-UA, за можливим винятком морського порту, в якому немає посадових осіб, які несуть цю відповідальність. Проблемним питанням є повідомлення про DoS-атаку Національній поліції через велику кількість заяв з різних джерел. Без чітких визначень проблем, про які слід повідомляти, вищим ешелонам влади буде складно забезпечити хорошу ситуативну обізнаність. Процедури, на які вони посилаються, насправді не написані, не поширені та не відпрацьовані командами на місці, наприклад, учасники згодні з тим, що щось на зразок 5 банків, що зазнали атаки, є пороговим значенням для звітності до Ради національної безпеки і оборони, але немає встановленого обмеження. Представники енергетичного і портового секторів не були присутні.

Коментарі до обговорення: Члени Синдикату підкреслили той факт, що Державна служба спеціального зв'язку та захисту інформації не представлена в адміністрації порту (але існують не секретні канали зв'язку). Команда вважає, що резервна інформація та процеси резервного копіювання дозволяють порту функціонувати. У порту працюють кілька експертів з кібербезпеки, але він не підключений до НКЦК. Також обговорювалися певні процедури, які повинні бути затверджені, щодо того, хто буде звітувати перед засобами масової інформації (це може бути НКЦК або ні), і роль постачальників програмного забезпечення в забезпеченні швидкої криміналістичної експертизи та відповідних рішень, коли надана певна інформація.

Ввідна 3.2.2: День 53: 27 лютого, 04:00

Є підозра про кібератаку на декілька компресорних станцій (КС) Південного транзитного коридору: Березівка (Одеська область), Павлоград (Дніпровська область) і Марівка (Миколаївська область), оскільки деяка дистанційно керована запірні арматура вишла з ладу, а оператори спостерігають неправильні показники датчиків. Потік транзитного газу в південно-східну частину Одеської області зупинений.

Реагування на Ввідну 3.2.2

Визначили, що CERT-UA стане першим органом реагування. СБУ поінформована і прийняла рішення про подальші дії, оскільки вони володіють цими об'єктами, адже вони є частиною антитерористичної інфраструктури.

Ефекти: Потік газу під час критичного холодного періоду порушений. Масштаби атаки та інші постраждали райони незрозумілі. Потенційна потреба в екстреному реагуванні в холодну пору року.

Необхідне реагування: СБУ керує цим процесом і має процедури, що включають розслідування джерел атаки. Вони вважають, що компресорну станцію можна відновити та зняти показники вручну. Для визначення наявності кібернетичного компонента в атаках залучені групи експертів-криміналістів. CERT-UA - це платформа для збору всієї інформації.

Проблемні питання (які перешкоджають ефективному реагуванню): Реалістичність/здійсненність сценарію з урахуванням особливостей підключення лічильників (аналогове підключення). Немає чітких ліній звітності. СБУ звітує перед Офісом Президента і незрозуміло, чи поширюється після цього інформація іншим людям. Остаточна домовилися про те, що CERT-UA є платформою збору даних (але тільки після довгої розмови). Вимоги щодо обміну інформацією про Показники компрометації (ІОС) не визначені належним чином.

Коментарі: Члени Синдикату обговорили реалістичність сценарію з урахуванням технічних деталей (наприклад, наскільки насправді можливе дистанційне керування запірною арматурою) і відзначили, що як засвідчує попередній досвід їм вдавалося виявляти кібератаки на газову систему і захищати її від зловмисників. Вони також заявили, що СБУ самостійно проводить розслідування і вирішує, кого інформувати про такі різні події, і що, ймовірно, будуть посилені заходи захисту через збільшений рівень загрози. Навчання, що проводяться СБУ, можуть включати або не включати кібертестування. Основна проблема функціонування та реагування СБУ на цю ввідну полягає в тому, що при реалізації заходів щодо запобігання терористичній діяльності СБУ часто не враховує кібер-складову в атаках такого роду. Також Державний центр кіберзахисту України на регулярній основі вживає заходів щодо тестування мереж критичної інфраструктури на наявність вразливостей. На

закінчення було рекомендовано, аби ці два види діяльності (заходи щодо запобігання терористичній діяльності та пентест (тестування проникнення)) здійснювалися спільно в ході розслідування.

Ввідна 3.2.3: День 53: 27 лютого, 09:00

Портові крани Liebherr в порту «Південний» не працюють (відмовила система управління кранами), неможливість організувати вантажно-розвантажувальні роботи, перспектива штрафних санкцій.

Реагування на Ввідну 3.2.3

Органами реагування повинні бути групи технічної підтримки на місці в порту і в Німеччині (але вони можуть бути недоступні). Цілком ймовірно, що порт спробує сам про все подбати та не повідомляти про те, що трапилось. Технічна команда в порту буде першою, хто відреагує. Перебої в роботі портів завдають економічної шкоди та призводять до великих фінансових втрат. Також можливі подальші міжнародні та страхові наслідки. Важливою формою реагування є інформування інших портових споруд про ознаки таких загроз. Зв'язатися зі службою підтримки та надати їм інформацію. Якщо атака є кібератакою, повідомити ДССЗ31/CERT-UA, повідомити Міністерство економіки та служби безпеки порту. При необхідності на національному рівні можна зв'язатися з компанією Liebherr. Стурбованість учасників полягає в тому, що служби безпеки кожного порту не мають процедур звітності вище. Якби існувала така процедура, то вони могли б проінформувати НКЦК, але зараз немає встановлених процедур для подібних ситуацій. Зрештою, є межі того, що можуть зробити місцеві кіберкоманди, тому стратегічні комунікації дуже важливі, поки рішення приймається в Німеччині.

Коментарі до обговорення: Учасники обговорили терміни та методи встановлення причини кібератаки та відповідні заходи реагування, враховуючи наявність іноземного обладнання. Вони також підкреслили той факт, що на об'єктах завжди знаходяться кіберкоманди та групи моніторингу, які стежать за роботою цього дуже дорогого обладнання, але вони, швидше за все, будуть розглядати ці проблеми з технічної точки зору, а не їх кібернетичний аспект. Одна з проблем, пов'язаних з цим сценарієм, полягає в тому, що це атака на технічну систему, що має захищене (приватне) програмне забезпечення (Liebherr).

Ввідна 3.2.4: День 54: 28 лютого, 14:00

«Укренерго» втрачає контроль над системою SCADA високовольтної мережі після оновлення системи. Критично важливі підстанції в Одеській області, такі як 750кВ Приморська, 330кВ Новоодеська, Трихати, Аджалик, відключені від мережі. Атака знищує дані у важливих системних файлах, що призводить до збою комп'ютерів.

Реагування на Ввідну 3.2.4

Державна компанія («Укренерго») має висококваліфіковану групу реагування і відреагує на цю ситуацію. У цій ситуації CERT.UA надасть загальні рекомендації. Це має величезний вплив на країну - від лікарень до вуличного освітлення. Всі системи, такі як водопостачання, відключені. На вулицях були б безлади. Це також зачепило б і міжнародні інтереси у зв'язку з експортом електроенергії у Велу. Окупаційні війська Бастана можуть використовувати це як привід для окупації. Одним зі способів реагування було б внутрішнє управління всією подією - автоматичне завантаження Показників компрометації до Платформи обміну інформацією про шкідливі програми (MISP) і відкат до попередньої стабільної версії програмного забезпечення. «Укренерго» інформує інші місця/галузі/ департаменти. Розгортання кібер команди експертів-криміналістів (від CERT.UA), аби визначити деталі атаки. Якщо є ознаки злочину, то в справу вступає СБУ. Уряд повинен надавати інформацію та допомогу в критично постраждалих цивільних районах. Група стурбована відсутністю

достатньої кількості експертів, підготовлених для реагування на ситуацію, це було одним з факторів, виявлених членами Синдикату. Офіцери, які займаються захистом критично важливих об'єктів інфраструктури, повинні бути навчені та найняті в мирний час для належного розгортання в кризових ситуаціях. Група військового реагування повинна співпрацювати з Державною службою спеціального зв'язку і захисту інформації (ДССЗІ) на постійній основі, аби перехід від військових дій до мирного часу не був переривчастим.

Коментарі для обговорення: Члени Синдикату зосередилися на можливому розміщенні військового персоналу для розв'язання цих проблем та на їх необхідній підготовці, навчанні та інтеграції в цивільний сектор. Також учасники обговорили необхідність введення надзвичайного та воєнного стану з відповідним розподілом обов'язків між Міністерством оборони та ДССЗІ щодо кіберзахисту критичної інфраструктури. Команда також детально вивчила подальші наслідки, зазначивши, що, ймовірно, в Одесі не буде води або електрики.

Відна 3.2.5: День 55: 1 березня, 00:00

Після оновлення декількох програмованих логічних контролерів (ПЛК) на Дністровській гідроакумулюючій електростанції зв'язок між виробничими процесами нестабільний. Оператор отримує нереалістичні дані про значення виробленої електроенергії. Крім того, раптово всі ворота підіймаються на максимальну висоту, викликаючи неконтрольований і незапланований витік води. Цей раптовий витік пошкоджує турбіни на гідроелектростанції, а також викликає швидку й масштабну повінь вниз по річці.



Реагування на Ввідну 3.2.5

Роль Державної служби з надзвичайних ситуацій визначається відповідно до Закону. Зрештою, Рада національної безпеки і оборони (РНБО) координуватиме дії з реагування на цю подію на національному рівні. В результаті масштабної повені будуть жертви. Довгострокові наслідки, економічні збитки, міжнародні проблеми (через експорт електроенергії) та наслідки для військової готовності та довгострокові наслідки для цивільного населення й промисловості. Про всі події буде проінформований Національний координаційний центр кібербезпеки. Буде прийнято рішення закликати Національну раду з безпеки і оборони спланувати та здійснити відповідні заходи на національному рівні. Члени Синдикату підкреслили відсутність належного реагування та кіберзахисту. Також було озвучено питання про негативний вплив на комплексну протиповітряну оборону в регіоні. Можливі командні навчання національного рівня (РНБО) за участю приватних, державних структур і збройних сил, які будуть заплановані до кінця цього року.

Коментарі до обговорення: Учасниками було підняте питання, чи це кібератака або акт військової агресії, і команда також зосередилася на обговоренні розгортання Збройних сил для надання допомоги в ліквідації наслідків катастрофи. Члени Синдикату обговорили можливість введення воєнного стану у відповідних регіонах.

Резюме учасників щодо Епізоду 3:

У цьому Епізоді підкреслювалася роль членів Синдикату в управлінні активами, оцінці вразливостей і зниженні/усуненні наслідків на місцевому, національному та міжнародному рівнях. Вимоги щодо обміну інформацією про Показники компрометації (ІОС) повністю визначені, і є 4 платформи обміну інформацією про шкідливі програми (MISP), але немає єдиної лінії звітності та набору вимог (учасники запропонували таке: Національна поліція > відділ кібербезпеки в Національній поліції > НКЦК > СБУ > Національна Рада оборони і безпеки (РНБО) > Президент). Необхідно також встановити процедури поширення інформації у зворотному напрямку і по горизонталі. Визначення кібератаки залишалось складним завданням - зокрема, терміни розслідування кібератак складають від декількох тижнів до декількох місяців, а збій у роботі пристроїв розглядається як фізичний до тих пір, поки не будуть виключені всі можливі причини, не пов'язані з кібератаками.

Розмова в синдикаті йшла більше про незалежну експертизу програмного забезпечення; практика експертизи програмного забезпечення в СБУ була визнана членами синдикату порочною, оскільки вона дозволяла контррозвідці займатися питаннями бізнесу, надаючи таким чином СБУ більше повноважень, ніж передбачено законом. Вимоги до проведення випробувань перед початком виробництва також були визначені як сфера, якій уряду необхідно приділяти більше уваги. Залучення Збройних сил - незабаром потрібно буде зробити більше для захисту критичної інфраструктури, а можливі командно-штабні навчання на національному рівні (РНБО) за участю приватних, державних структур і збройних сил, які будуть співпрацювати до кінця цього року, були запропоновані як наступні кроки.



4.4. Епізод 4: Гібридна війна

Напруженість у відносинах між Бастаном і Сентою досягла найвищого рівня за всю їх історію. Військова розвідка Сенти повідомила про безпрецедентне нарощування військових сил і засобів на базах Бастанського флоту в морі Нуар. На острові Тотара почала відбуватися значна кількість провокаційних нещасних випадків. Повідомлення про втрату сигналів GPS і GSM на острові. Підключення до Інтернету на острові зникло.

У той самий час Сента продовжує стикатися зі збільшенням кількості кібератак на урядові та місцеві установи та постачальників критично важливих послуг. ЗМІ Бастана і Сенти повідомляють в агресивній манері про нездатність центральної та місцевої влади Сенти надавати населенню критично важливі послуги. Більш того, вищі командири Збройних сил Сенти в Києві та посадові особи Військово-морських сил в Одесі та на острові Тотара отримали електронні листи з непідтверджених профілів з прямим попередженням «не виконувати накази політичного керівництва Сенти, інакше вони та їхні сім'ї будуть у небезпеці».

Соціальні мережі сповнені повідомлень і активних дискусій про можливе відділення південної частини Сенти. Ті ж новини поширюються через офіційні вебсторінки регіональних рад. Все вищевказане призводить до тиску та напруження всередині державних установ, правоохоронних органів і збройних сил. За останні 24 години різко посилюються вуличні демонстрації проти уряду Сенти, а саме в центральних містах південних регіонів: Одесі, Миколаєві та Херсоні. В результаті уряд функціонує на межі можливого, а населення збентежене.

На тлі значних кібератак, психологічного тиску, поширення дезінформації і дедалі більших вуличних протестів у південних регіонах на острові Тотара раптово висадилася значна кількість о/с збройних сил без розпізнавальних знаків. Доступ до порту острова Тотара заблокований вантажними суднами без розпізнавальних знаків і прапора держави. Доступ по воді до острова Тотара відрізаний. Бурові

установки для видобутку вуглеводнів на острові Тотара, розташовані у ВЕЗ Сента, були захоплені й тепер знаходяться під повним контролем озброєних людей без розпізнавальних знаків.

Реагування на Епізод 4

Цей Епізод пропонував серйозні кібератаки, радіоелектронну війну та введення воєнного стану. Він також створював виклики для проведення оцінки групою через недостатність знань щодо дій уряду під час гібридної атаки – те, з чим учасники були набагато краще знайомі. Пояснення конкретних процедур і положень в рамках воєнного стану, які застосовуються військовими, були описані як події, які відбулися попередньо та подібні описаним у Ввідній 1. У цьому випадку Одеська/обласна рада не виконувала накази військових, і було детальне обговорення того, що робити з місцевими адміністраціями, які не виконують накази. Команда також зробила розрізнення між місцевим та національним рівнями воєнного стану.

Ввідна 4.2.1: День 56: 2 березня, 10:00

Є підозра про значну кібератаку на основні інтернет-провайдери Сенти. Підключення до Інтернету на острові Тотара повністю відсутнє.

Реагування на Ввідну 4.2.1

Основним органом реагування будуть військові (у зв'язку з введенням воєнного стану) та буде підтримка з боку Державної служби спеціального зв'язку та захисту інформації. Безпосередні наслідки полягають в тому, що інтернет з'єднання на острові Тотара повністю відсутнє, що призводить до паніки, безладів і порушення економічних і цивільних операцій, а також до початкового потенційного порушення деяких військових комунікацій. Реагування повинне виконуватися Державною службою спеціального зв'язку та захисту інформації, яка має у своєму розпорядженні ресурси для забезпечення інших форм зв'язку з островом. Військові можуть також забезпечити інші форми зв'язку з островом. Військові отримають інструкції від військової адміністрації та направлять місцеві цивільні та військові активи для розв'язання проблеми. Мета - це поширення інформації протягом однієї години серед усіх установ. Важливими питаннями є такі: чи це коли-небудь відпрацьовувалося або робилося? Наскільки важливим є інтернет зв'язок на цьому острові? Військові нададуть друковані копії, якщо зв'язок буде перерваний (але неясно, як це координується в необхідному масштабі). Додавання положень до проєкту закону про кібербезпеку для визначення того, як місцеве військове командування буде звітувати перед урядом і координувати свої дії з ним.

Коментарі до обговорення: Робоче припущення полягає в тому, що інтернет з'єднання дійсно ушкоджене, як описано у сценарії, і що в Одеській області введено воєнний стан. Учасники зазначили, що Державна служба спеціального зв'язку та захисту інформації має ресурси для забезпечення інших форм зв'язку на острові.

Ввідна 4.2.2: День 58: 4 березня, 16:00

На корабельно-катерному складі Одеського загону морської охорони регіонального управління морської безпеки Державної прикордонної служби Сенти були пошкоджені навігаційні системи.

Реагування на Ввідну 4.2.2

Першим органом реагування буде Державна служба спеціального зв'язку та захисту інформації, оскільки передбачається, що це випадок радіоелектронної боротьби. Деякі видимі безпосередні наслідки – це економічний і міжнародний репутаційний збиток, а також плутанина. Важливим першим кроком було б знайти і нейтралізувати джерело перешкоди/ підміни сигналу.

Є занепокоєння з приводу відсутності процедур запобігання перешкодам і підміні сигналів GPS/AIS. На національному рівні немає жодних процедур для обробки інформації, що надходить в міжнародну мережу.

Коментарі до обговорення: Це продовження питання про зіткнення суден (можливо). Після попереднього інциденту вони повинні були мати більш надійний план запобігання в подібних випадках. Ніхто в цьому синдикаті не є експертом у сфері морської безпеки, особливо в питаннях GPS.

Відна 4.2.3: День 59: 5 березня, 10:00

Острів Тотара втрачає сигнали GPS і GSM. Водночас на вебсайті парламенту Тотари повідомляється, що з метою захисту місцевого населення від геноциду з боку ультраправих угруповань Сенти влада острова приймає рішення оголосити про відокремлення від Сенти та звертається до Бастана за допомогою.



Реагування на Ввідну 4.2.3

Військова адміністрація та СБУ (пропозиція про введення воєнного стану) повинні відреагувати на цю ситуацію. Аерокосмічне агентство також може бути залучене до розслідування проблеми з GPS. Відділ державного контролю Державної служби спеціального зв'язку та захисту інформації. Безпосередні наслідки ситуації включають плутанину і хаос на материк, потенційне насильство, конфронтації та заворушення. Перехід до ведення бойових дій і введення воєнного стану в певних регіонах. Після розслідування СБУ повинне зробити оголошення для громадськості про те, що інформація є фальшивкою. Після 2014 року були зроблені певні дії, тому тепер існують дуже чіткі процедури щодо кроків, які будуть зроблені у випадку територіальних проблем, подібних до цієї. Для приватного сектора необхідно усунути неполадки та відновити GSM. Розташування острова таке, що операції можуть проводитися з позицій сили, а це означає набагато меншу ймовірність відділення й виходу зі складу країни. Необхідні додаткові тренування й навчання, аби впоратися з потенційним відділенням(и) (виходом зі складу країни). Незрозуміло, хто буде ключовим персоналом для відновлення мережі GSM. Немає чітких інструкцій щодо того, як розподілити контроль.

Коментарі до обговорення: Члени Синдикату висловили побоювання з приводу можливої диверсійної атаки на стільникову мережу, як це було під час конфлікту на Донбасі. Звичайні громадяни, швидше за все, не матимуть доступу до інформації - на материк громадяни можуть бути обізнані про те, що відбувається, але на острові люди можуть і не знати всієї інформації. У регіонах, де введено воєнний стан, військовослужбовцям тепер дозволено користуватися стільниковим зв'язком.

4.5. Епізод 5: Посткризова стабілізація

Цей епізод присвячений посткризовому відновленню та процесу стабілізації. Посткризова стабілізація відбувається після закінчення кризового сценарію – з 7 березня 20XX року. Також потрібно обговорити питання управління в кризових ситуаціях.

Кожному синдикату буде запропоновано кілька питань для обговорення посткризової стабілізації.

Будь ласка, обговоріть і дайте відповідь на вказані нижче питання:

1. Як ви бачите концепцію оновлення/розробки заходів та планів кібербезпеки для наявної системи?

Відповідь

Головним обговорюваним кроком була концепція національної стійкості. Цей закон був написаний і очікує затвердження президентом. Це дозволило б українському уряду запустити правовий механізм для систематичного нарощування заходів щодо стійкості (в тому числі кіберстійкості). Відсутність затвердженого списку об'єктів КІ була проблемою для розробки планів, а постанова Кабінету Міністрів вимагає визначення об'єктів КІ, але її ще не виконали. Ще одна проблема, виявлена учасниками, полягає в тому, що в міністерствах мало експертів, які могли б зосередитися на цих питаннях.

Крім того, не існує Національного плану реагування на кіберзагрози. Усі учасники обговорення погодилися з тим, що існує нагальна необхідність введення посад офіцера з

інформаційної безпеки (CISO) в урядових установах, державних і приватних організаціях. Загальне кримінальне право допускає широке коло обов'язків, тому для КІ потрібен спеціальний закон про кібербезпеку, враховуючи її важливість.

2. Чи достатньо всеосяжним (компетентним) на сьогодні є законодавство у сфері забезпечення та розвитку кібербезпеки? Якщо ні, то які пріоритетні області для його поліпшення в посткризовому аналізі?

Відповідь

На державному рівні відсутня практика оцінки ризиків у кіберпросторі. Державно-приватне партнерство є пріоритетом, при цьому також використовуються канали соціальних мереж для надійної комунікації з населенням - наприклад, розміщувати відеоролики та пояснювати речі «простими словами» і аналізувати випадки таким чином, аби ними можна було поділитися з населенням в цілому, оскільки населення потребує своєчасної інформації та прозорості.

Повноваження Збройних Сил, Державної служби спеціального зв'язку та захисту інформації та приватного сектора на різних етапах кризи повинні бути визначені чіткіше.

3. Сьогодні провідні компанії та фахівці в області кібербезпеки зосереджені на створенні багаторівневих інтегрованих систем безпеки, основним принципом яких є попереджувальне управління кібер ризиками з урахуванням стратегічних цілей організації (об'єкт захисту), з одного боку, і змін в спектрі кіберзагроз, з іншого боку. Яким чином дотримання вимог кібербезпеки має бути інтегроване в стратегію (заходи) захисту критичної інфраструктури?

Відповідь

Учасники зосередили свою увагу на законодавстві у сфері кібербезпеки. Пріоритети включають визначення рівня кіберзагроз та проведення аудитів кіберзахисту, включаючи КІ. Було виявлено ряд джерел даних і проблемних питань, таких як:

- Дані ДССЗЗІ
- Дані незалежних аудитів (проблематично, оскільки нині немає незалежних аудитів /немає механізмів для цього)

Примітно, що ДССЗЗІ знайшла вихід, використовуючи «Оксфордську модель» замість законодавства: Модель зрілості можливостей кібербезпеки для країн (СММ). Посилання: <https://gcscc.web.ox.ac.uk/cmm-dimensions-and-factors#/>. У приватному секторі підприємства повинні проводити власні аудити, але уряд повинен надати інструкції, вимоги і рекомендації (передовий досвід).

4.6. Ключові висновки

Коли застосовувався контроль з боку військових на місцевому або національному рівні, то учасники не були впевнені в обов'язках свого відомства. Не були повністю розглянуті питання стосовно того, як військові використовуватимуть невійськові та цивільні кіберресурси (наприклад, всі невійськові активи) у разі введення воєнного стану. Крім того, координація між військовими та цивільними

ресурсами була неясною – учасники відзначили, що в умовах воєнного стану держава може отримати будь-які ресурси зв'язку в інтересах національної безпеки, але є питання про те, як приватні оператори збираються співпрацювати в цих умовах.

Крім того, члени Синдикату підняли тему наявності кібер-резерву. Нині існують процедури, які визначають очікувану кількість співробітників кібер-резерву для реагування на різні ситуації, однак для зарахування членів як солдат кібервійськ їм необхідно мати посаду, офіційно затверджену і санкціоновану урядом, а цього ще не було зроблено.



Вимога про проведення незалежної оцінки управління активами. Стратегія кібербезпеки України, затверджена Указом Президента України № 96 від 15 березня 2016 року, поклала початок зусиллям зі створення і розвитку національної системи кібербезпеки, проте нині кожне відомство будує свою власну структуру, оскільки немає комплексного законодавства. Відсутність законодавства ускладнює зусилля на національному рівні та створює дублювання функцій у багатьох відомствах. На сьогодні не було успішно проведено жодної незалежної оцінки управління активами, оцінки вразливості та зменшення/усунення наслідків. **Рекомендація:** Національний центр кібербезпеки (НКЦК) та команда реагування на комп'ютерні надзвичайні ситуації України (CERT-UA) або формально розробляють структуру кібербезпеки, або приймають наявну структуру для виконання управління оцінкою, побудови системи оцінювання вразливостей і створення методів зменшення наслідків для підвищення стійкості.

Вимога централізації роботи чотирьох Платформ обміну інформацією про шкідливі програми. Існує чотири Платформи обміну інформацією про шкідливі програми (MISP), які не сумісні або не пов'язані між собою, керовані різними урядовими та розвідувальними агентствами. Крім того, в

Україні немає стандартних Показників компрометації (IOC) атак у всіх державних структурах. **Рекомендація:** Централізація роботи чотирьох Платформ обміну інформацією про шкідливі програми (MISP) підвищить сумісність і взаємозв'язок між урядовими/розвідувальними агентствами. Крім того, ми рекомендуємо стандартизувати Показники компрометації (IOC) для уряду та міжнародних партнерів.

Вимога про створення національних кібер-резервів. Під час численних кризових епізодів застосовувався контроль з боку військових на місцевому або національному рівні, а учасники не були впевнені в обов'язках свого відомства. Не були повністю розглянуті питання стосовно того, як військові використовуватимуть невійськові та цивільні кіберресурси (наприклад, всі невійськові активи) у разі введення воєнного стану. Основні спроможності інших державних підприємств і компаній не були повністю оцінені або показані в планах реагування. **Рекомендація:** Створити національні кібер-резерви. У країні відсутня концепція резерву кібервійськ, а враховуючи специфіку підготовки, з цим необхідно визначитися в мирний час (і пройти поглиблену підготовку у військових сценаріях). Це також забезпечить призов солдатів в спеціальні підрозділи, де їх навички можуть бути використані найкращим чином, і дозволить налагодити міцне державно-приватне партнерство (ДПП) для проведення навчань у мирний час.

Вимога щодо впровадження управління електронними доказами. В інтернет провайдерів відсутній експертно-криміналістичний збір доказів цифрових злочинів у декількох сферах. Коли відбувається цифровий злочин, має проходити серія подій зі збору даних (що зветься ланцюжком забезпечення збереження зібраних даних), аналогічних тим, які передують цивільному або кримінальному переслідуванню, але зараз цього не відбувається. Найбільш помітним з них, зокрема, є послідовний метод збору та зберігання судових доказів від інтернет-провайдерів. Крім того, не існує правової норми про мінімальний термін, протягом якого інтернет провайдери зберігають дані, що проходять через їх мережу. Зараз процеси збору даних, аналогічні цивільному або кримінальному процесу, не узгоджені між правоохоронними органами та інтернет провайдерами. Цифровий збір доказів, перевірка цифрових доказів та експертно-криміналістичне визначення зловмисника(ів) (будь то людини або автоматизованої системи атаки) нині систематично не фіксуються. Україна ратифікувала Будапештську конвенцію (Верховна Рада - парламент), але не виконала положення Конвенції в повному обсязі. Стаття 20 Будапештської Конвенції говорить, що необхідно ратифікувати національний вторинний нормативно-правовий акт. Відповідно до цього не існує єдиної правової норми для збору експертно-криміналістичних даних/доказів від постачальників даних. **Рекомендація:** Кабінету Міністрів слід розробити стандартизований метод (як і що) збору та зберігання цифрових даних інтернет провайдерами (спільно з правоохоронними органами). Він повинен регулювати, які дані повинні збиратися і яким чином вони повинні зберігатися. Забезпечити навчання співробітників правоохоронних органів разом з усім персоналом, залученим до провадження, щодо особливостей цифрових доказів (допустимість, зміст), аби довести цифрове кримінальне провадження до кінця і досягти результатів. Законодавство про збір цифрових доказів має бути введено в дію в найближчому майбутньому, аби забезпечити послідовний збір даних інтернет провайдерами. Для інтернет провайдерів повинні бути встановлені мінімальні часові рамки в дев'яносто днів для зберігання даних сеансу, оскільки ці дані містять важливу інформацію про передбачуваного зловмисника (зловмисників).

5. Синдикат 3: Морська безпека

5.1. Епізод 1: Доконфліктна фаза: Гібридний вплив

Посилюється політичне та економічне залякування з боку влади Бастана. На підставі угоди про транзит газу, яка була підписана між Бастаном і Сентою минулого року, уряд Бастана звинуватив Сенту в порушенні положень угоди. Сента заперечує будь-які порушення. Однак ЗМІ Бастана і деякі ЗМІ Сенти, контрольовані Бастаном, продовжують поширювати повідомлення про порушення Сенти, підкреслюючи важливість відповідної угоди для енергетичної безпеки Європи, оскільки транзит газу в європейські країни частково забезпечується через територію Сенти.

Ситуацію ускладнює той факт, що між Бастаном і Велою не укладено новий контракт на постачання газу. Враховуючи суперечки щодо договірних положень, Бастан тимчасово істотно скорочує постачання газу в Велу. Вела максимально відбирає газ з транзитного трубопроводу, обмежуючи постачання газу споживачам Сенти в Одеській області, недалеко від кордону з Румунією.

Тим часом Бастан ввів обмеження на імпорт сільськогосподарських, промислових товарів і металевих виробів, палива, хімікатів і нафтопродуктів із Сенти. Крім того, Бастан припиняє постачати нафтопродукти в Сенту автомобільним, залізничним транспортом і трубопроводами.

В Інтернеті були виявлені три вебсайти з ідентичним візуальним оформленням і функціями офіційних вебсайтів Оператора ГТС Сенти, Оператора PSG і компанії «Нафтогаз». Крім того, на електронні адреси регіональних урядових установ Сенти були надіслані листи з фішинговими функціями та прикріплені текстові документи Microsoft Word.

У ЗМІ з'явилися повідомлення про потужну кібератаку на внутрішню мережу Liebherr в Німеччині. В результаті портові крани в морському порту Поті в Зестані перестали працювати.

З середини грудня берегова охорона Сенти регулярно повідомляє про присутність Військово-морських сил Бастана у ВЕЗ Сенти. Повідомляється, що Бастан проводив військові навчання в морі Нуар у безпосередній близькості від фарватерного проходу торгових і пасажирських суден з/в порти Одеської області.

Реагування на Епізод 1

Учасники обговорювали, чи були операції ВМС Бастана у ВЕЗ Сенти порушенням (невідомого) національного законодавства та/або міжнародного права. У той час як учасники погодилися, що прикордонна служба несе відповідальність за розробку і виконання плану реагування (у тому числі надсилання запиту щодо додаткових сил), синдикат не обговорював військові спроможності та потенціал кораблів ВМС Бастана у порівнянні зі спроможностями і потенціалом Держприкордонслужби. У спробі запобігти додатковій агресії з боку ВМС Бастана учасники схвалили виділення додаткових сил для забезпечення захисту критичної інфраструктури.

Координаційна нарада під керівництвом Антитерористичного центру полегшила б завдання Національної гвардії, Національної поліції та пов'язаних з ними служб внутрішньої безпеки щодо встановлення жовтого рівня загрози для постраждалих регіонів.

У відповідь на виявлення вибухового пристрою учасники домовилися, що прикордонна служба буде пропускати судна/катери з території Одеського загону Морської охорони під час розслідування.

Зокрема, учасники погодилися з тим, що буде необхідне рішення політичного керівництва для реагування на спроби Військово-Морських сил Бастана зупинити танкер. Крім того, політичне керівництво має вирішити, чи слід доручати морській охороні Державної прикордонної служби Сенти (або альтернативній службі) супроводжувати комерційні судна, що прибувають/відбувають з портів Сенти.

Хоча учасники не розглядали безпосередньо дії ВМС Бастана, вони були позначені такими термінами по всьому Епізоді: «провокаційні», «порушення», «порушення свободи судноплавства», «перешкоджання судноплавству» і «агресивні». Учасники чітко не сформулювали, які департаменти/відомства відповідають за розгляд кожного терміна відповідно до національного законодавства Сенти та розмежування визначення (наприклад) «провокації» і «агресивних дій». Учасники виявили проблеми з визначенням певних термінів у національному законодавстві, таких як «провокації», «агресивні дії».

Ввідна 1.3.1: День 5: 10 січня, 10:00

Присутність Військово-морських сил Бастана у ВЕЗ Сенти значно збільшилася за останні тижні. Деякі кораблі ВМС маневрують в прилеглий зоні Сенти та не відповідають на запити берегової охорони Сенти про ідентифікацію та надання інформації.

Реагування на Ввідну 1.3.1

Учасники обговорювали, чи були операції ВМС Бастана у ВЕЗ Сенти порушенням (невідомого) національного законодавства та/або міжнародного права. У той час як учасники погодилися, що прикордонна служба несе відповідальність за розробку і виконання плану реагування (у тому числі надсилання запиту щодо додаткових сил), синдикат не обговорював/не дискутував щодо військових спроможностей і потенціалу кораблів ВМС Бастана у порівнянні зі спроможностями та потенціалом Держприкордонслужби. У спробі запобігти додатковій агресії з боку ВМС Бастана учасники схвалили виділення додаткових сил для забезпечення захисту критичної інфраструктури.

Ввідна 1.3.2: День 11: 16 січня, 08:00

На стоянці корабельно-катерного складу Одеського загону Морської охорони виявлено вибуховий пристрій. Чергова служба Державної прикордонної служби Сенти починає розслідування.

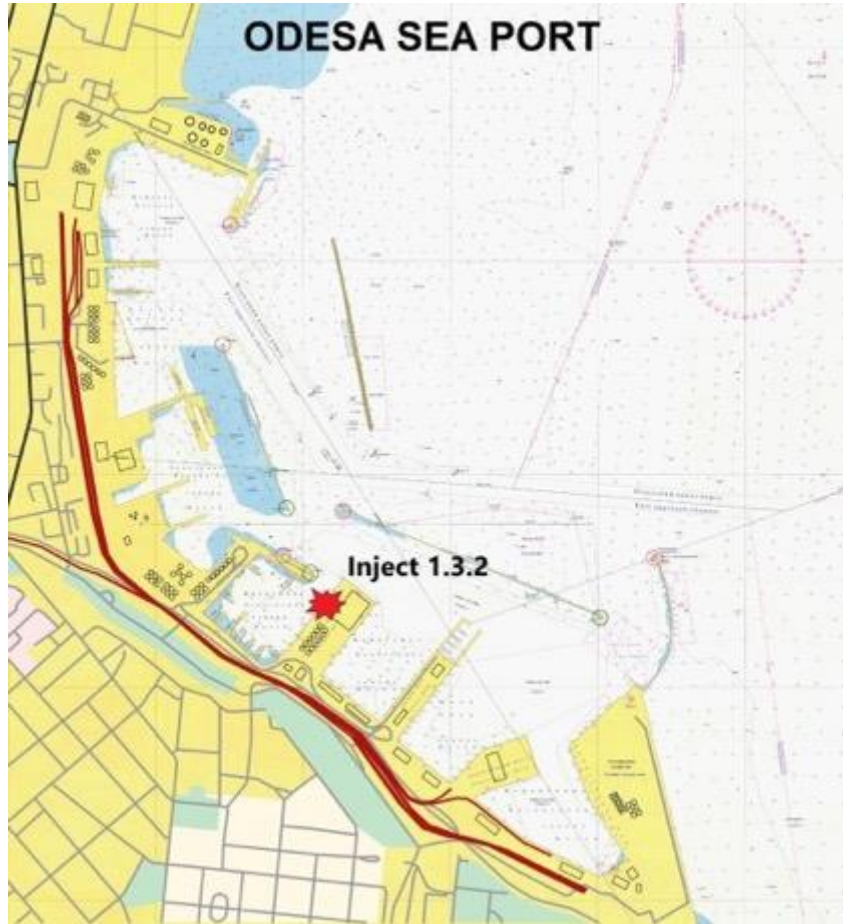
Реагування на Ввідну 1.3.2

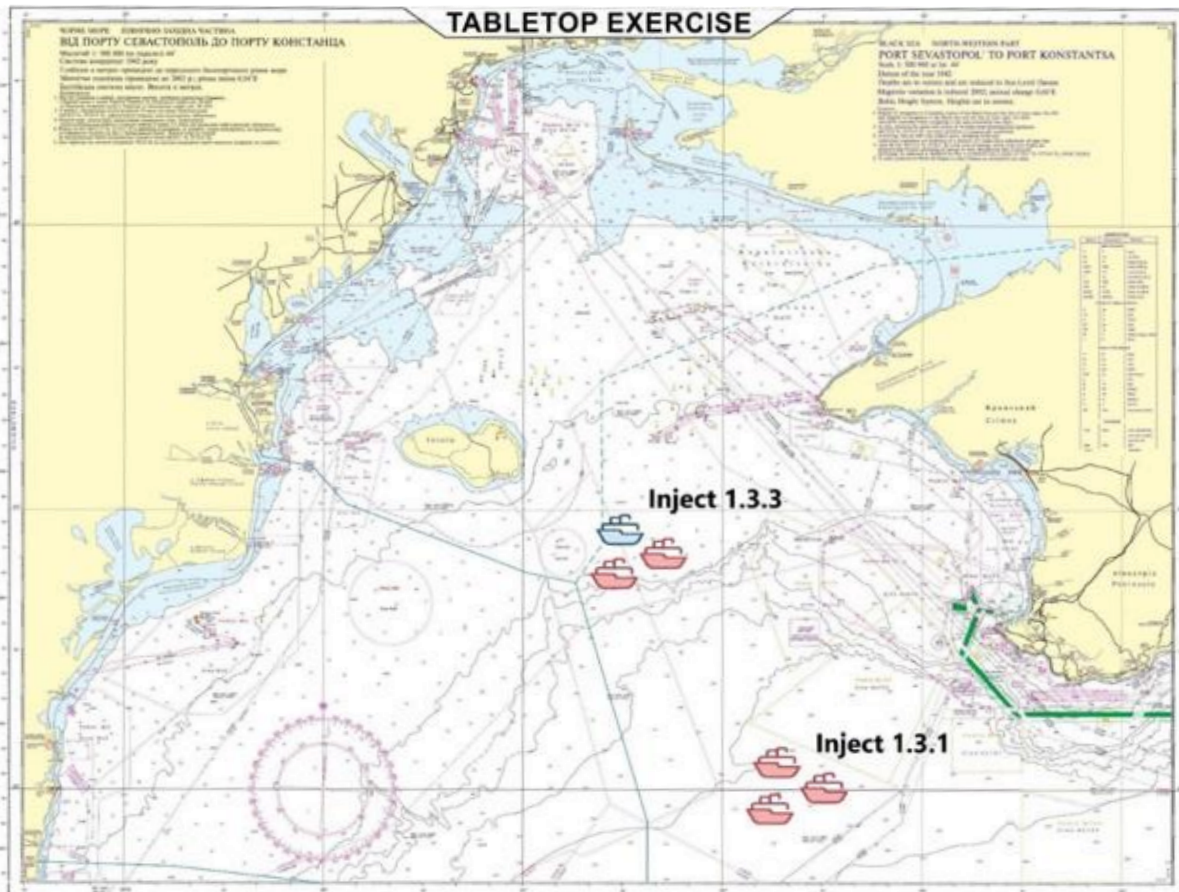
Координаційна нарада під керівництвом Антитерористичного центру полегшила б завдання Національної гвардії, Національної поліції та пов'язаних з ними служб внутрішньої безпеки щодо встановлення жовтого рівня загрози для постраждалих регіонів.

У відповідь на виявлення вибухового пристрою учасники домовилися, що прикордонна служба буде пропускати судна/катери з території Одеського загону Морської охорони під час розслідування.

Ввідна 1.3.3: День 19: 24 січня, 12:00

Група кораблів ВМС Бастана намагається зупинити танкер, що йде під прапором Сенти в Одеський морський порт, під приводом «проведення безпекової операції». Використовуються заклики та попередження, що надсилаються по каналах зв'язку.





Реагування на Ввідну 1.3.3

Зокрема, учасники погодилися з тим, що буде необхідне рішення політичного керівництва для реагування на спроби Військово-Морських сил Бастана зупинити танкер. Крім того, політичне керівництво має вирішити, чи слід доручати морській охороні Державної прикордонної служби Сенти (або альтернативній службі) супроводжувати комерційні судна, що прибувають/відбувають з портів Сенти.

Хоча учасники не розглядали безпосередньо дії ВМС Бастана, вони були позначені такими термінами по всьому Епізоді: «провокаційні», «порушення», «порушення свободи судноплавства», «перешкоджання судноплавству» і «агресивні». Учасники чітко не сформулювали, які департаменти/відомства відповідають за розгляд кожного терміна відповідно до національного законодавства Сенти та розмежування визначення (наприклад) «провокації» і «агресивних дій».

5.2. Епізод 2: Гібридні операції низької інтенсивності

На початку лютого погодні умови в південних районах Сенти погіршилися. Швидкість вітру досягає 50 м/с, що завдає значної шкоди, зокрема, в Одеській області.

Введені Бастаном обмеження на імпорт товарів сільського господарства, обробної промисловості та металевих виробів, палива, хімікатів і нафтопродуктів із Сенти сприяють занепаду економіки Сенти, яка вже знаходиться в стані рецесії. Пробастанські активісти використовують економічний спад як шанс посилити протести проти уряду Сенти. Соціальна напруженість досягла свого піка, коли в Інтернеті поширилася новина про рішення Одеської міської ради про вихід Одеської області зі складу Сенти.

Діяльність пробастанських активістів та інцидентами у сфері кібербезпеки постійно порушують роботу Одеського морського порту. Крім того, цивільні судна і кораблі берегової охорони Сенти повідомляли про технічні неполадки у роботі своїх навігаційних систем.

Крім того, судна Бастана діють агресивно проти риболовецьких суден Сенти. Кораблі берегової охорони Бастана залякують і погрожують вантажним суднам Сенти, а також суднам іноземних держав. Нещодавно Військово-морські сили Бастана надали підтримку незаконній діяльності з розвідки газу та встановлення бурових установок на території ВЕЗ Сенти. Навколо бурових установок був встановлений цілодобовий охоронний патруль Військово-морських сил Бастана.

Реагування на Епізод 2

Всі учасники колективно погодилися, що Сента повинна забезпечувати безпеку судноплавства в територіальних водах, у тому числі виключна економічна зона (ВЕЗ). Учасники мали різні точки зору щодо того, як Сента досягне цієї мети. Повторюваною темою в ході обговорень було визначення того, який департамент/відомство/збройні сили Сенти буде (-уть) керувати скоординованим реагуванням і відповідно до якого закону/повноважень. Було вирішено, що Морська охорона Прикордонної служби Сенти буде виявляти розливи нафти та інші подібні інциденти, а рятувальні заходи та операції реагування будуть проводитися Державною службою з надзвичайних ситуацій спільно з Міністерством інфраструктури у співпраці з іншими відповідними відомствами.

Синдикат розцінив дії бастанських ВМС і берегової охорони як навмисні та такі, що спрямовані на створення негативного іміджу Сенти як морської держави, які матимуть негативний вплив на її економіку.

Учасники погодилися з тим, що Міністерство закордонних справ (МЗС) очолить зусилля щодо звернення до міжнародної спільноти за допомогою. МЗС буде доручено: дипломатичним чином запобігти подальшій ескалації конфлікту (конфліктів), використовувати міжнародне право і підтримку з боку міжнародної спільноти, аби змусити Бастан визнати та припинити діяльність у ВЕЗ Сенти, та спробувати уповільнити операції Бастана, аби збільшити час для прийняття рішень політичним керівництвом Сенти. Тим часом учасники в цілому підтримали ідею збільшення кількості сил оборони на острові Тотара як превентивний захід.

Ввідна 2.3.1: День 26: 31 січня, 10:00

Кілька цивільних кораблів Сенти та кораблів берегової охорони в морі Нуар неподалік Одеського морського порту повідомляють про аномалії з їх позиціонуванням за допомогою GPS. Про подібні перешкоди повідомляють цивільні кораблі Зестану. Оператори повітряного простору Сенти

повідомляють про втрату сигналів від деяких пасажирських літаків, що пролітають над узбережжям Сенти в морі Нуар. У ВЕЗ Сенти виявлено судно під прапором Коморських островів, що здійснює радіоелектронну боротьбу і розвідувальну діяльність в інтересах Бастана.

Реагування на Ввідну 2.3.1

Всі учасники колективно погодилися, що Сента повинна забезпечувати безпеку судноплавства в територіальних водах, у тому числі виключна економічна зона (ВЕЗ). Учасники мали різні точки зору щодо того, як Сента досягне цієї мети.



Синдикат морської безпеки обговорює проблемні питання в «Морі Нуар» під час КШН «НАТО CORE 20» в Одесі, Україна.

Ввідна 2.3.2: День 43: 17 лютого, 10:00

Танкер, що належить Сенті, раптово втрачає управління і стикається з вантажним судном Бастана у ВЕЗ Сенти, що призводить до витоку нафти та великої пожежі. Повідомляється про декількох постраждалих. Влада Бастана звинувачує владу Сенти в диверсії.

Реагування на Ввідну 2.3.2

Повторюваною темою в ході обговорень було визначення того, який департамент/відомство/Збройні сили Сенти буде/уть/ керувати скоординованим реагуванням і відповідно до якого закону/повноважень. Було досягнуте взаєморозуміння, що Морська охорона Прикордонної служби Сента буде керувати рятувальними операціями та реагувати на розлив нафти. Примітно, що учасники вперше в ході навчань згадали про використання Військово-Повітряних сил для підтримки пошуково-рятувальних операцій (в очікуванні схвалення політичним керівництвом).

Ввідна 2.3.3: День 46: 20 лютого, 17:00

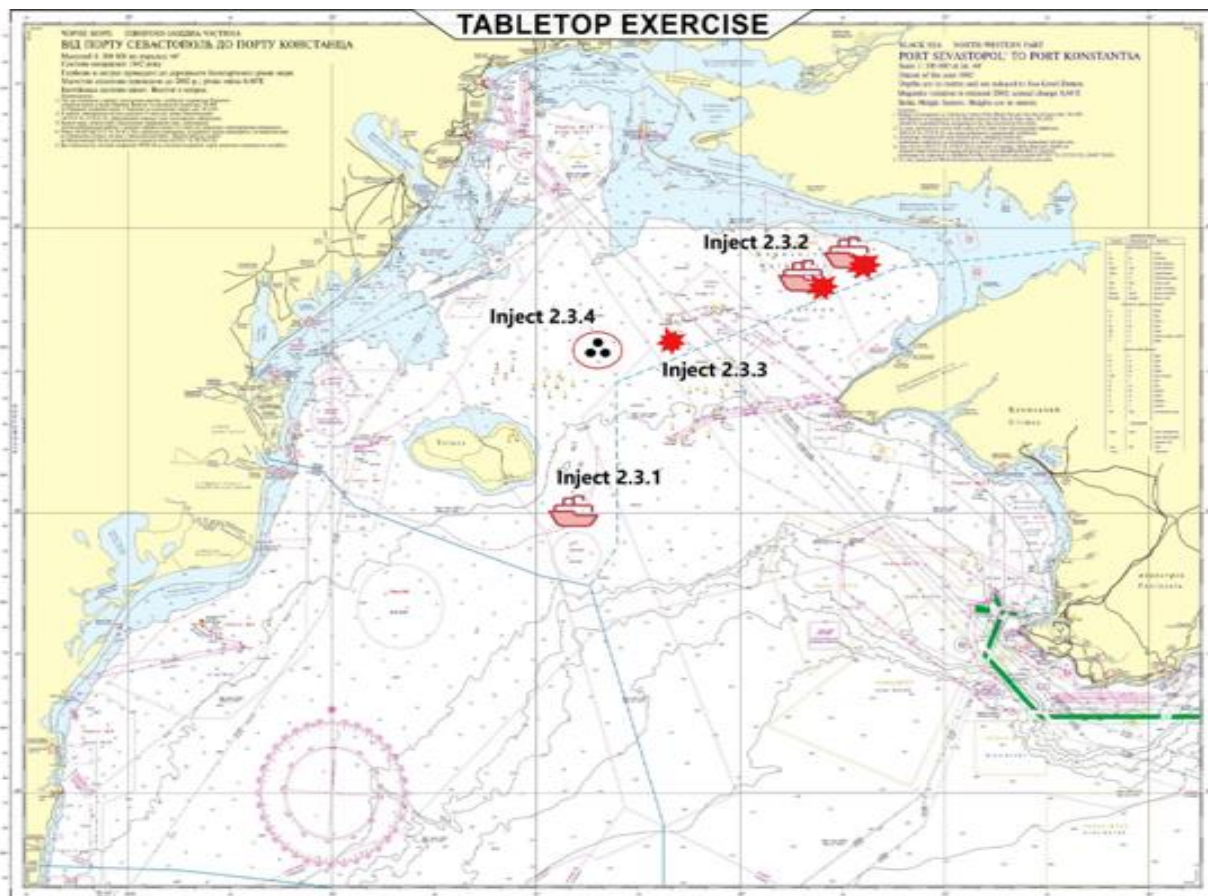
Кораблі берегової охорони Сенти інформують про дії ВМС Бастана в морі Нуар. Останнім часом Бастан розпочав установку газових самопідйомних бурових установок на території континентального шельфу Сенти. Кораблі ВМС Бастана патрулюють навколо цих газових вишок.

Реагування на Ввідну 2.3.3

Синдикат розцінив дії бастанських ВМС і берегової охорони як навмисні та такі, що спрямовані на створення негативного іміджу Сенти як морської держави та що матимуть негативний вплив на економіку.

Ввідна 2.3.4: День 48: 22 лютого, 07:00

Військово-Морські сили Бастана і берегова охорона залякують цивільні вантажні судна Сенти та Зестану, що прямують в порти Сенти в морі Нуар, перебуваючи у ВЕЗ Сенти, і вимагають, аби вони змінили курс назад до зовнішнього кордону ВЕЗ Сенти. Згідно з даними ЗМІ Бастана, цивільний вантажний корабель Сенти навмисно намагається врізатися в корабель ВМС Бастана. Згідно з повідомленнями ЗМІ Бастана, за таких обставин влада Бастана вирішила збільшити свою військово-морську присутність, аби захистити свої кораблі та інтереси від провокаційних дій Сенти.



Реагування на Ввідну 2.3.4

Учасники погодилися з тим, що Міністерство закордонних справ (МЗС) очолить зусилля щодо звернення до міжнародної спільноти за допомогою. МЗС буде доручено: запобігти подальшій ескалації конфлікту (конфліктів), використовувати міжнародне право і підтримку з боку міжнародної спільноти, аби змусити Бастан визнати та припинити діяльність у ВЕЗ Сенти, та спробувати уповільнити операції Бастана, аби збільшити час для прийняття рішень політичним керівництвом Сенти. Тим часом учасники в цілому підтримали ідею збільшення кількості сил оборони на острові Тотара як превентивний захід.

5.3. Епізод 3: Фаза конфлікту: Гібридні операції високої інтенсивності

Критична інфраструктура Сенти піддається широкому спектру ударів кінетичною і некінетичною зброєю. Перебої в роботі газопроводу з транспортування природного газу в Південному газотранспортному коридорі позначаються на постачанні газу в Південний регіон Сенти та сусідні іноземні держави. Більш того, існує загроза зриву опалювального сезону не лише в південній частині Сенти, але й у Харківській і Луганській областях, які, зокрема, сильно залежать від постачання газу з Бастана.

На півдні Сенти на третину збільшилася кількість надзвичайних ситуацій, пожеж і нещасних випадків, викликаних підпалами й терористичними актами з використанням вибухових речовин, що, своєю чергою, призвело до значного збільшення числа постраждалих. Є підозра про масштабний інцидент на ПАТ «Одеський припортовий завод», де повідомляється про значний викид небезпечних хімічних речовин.

Поширюється інформація про збій в роботі Південно-Сентської АЕС. ЗМІ Бастана звинувачують владу Сенти у викидах радіації. Майже одночасно поширюється інформація про атаку на гідроакумулюючу електростанцію.

Масовані кібератаки порушують роботу Одеського морського порту, в тому числі транспортування й обробку вантажів. Нападу зазнали банківські системи відділень Ощадбанку і ПриватБанку в Одеській області.

Через місяць після першої кібератаки на внутрішню мережу Liebherr в Німеччині сталася серія незначних кібератак на портові крани Liebherr по всій Європі.

У морській сфері кораблі ВМС Бастана збільшують свою присутність у ВЕЗ Сенти, використовуючи Військово-морські навчання, припиняючи міжнародні морські перевезення пасажирів і вантажів.

Реагування на Епізод 3

Члени Синдикату одностайно погодилися з тим, що дії Бастана ілюструють очевидну мету завдати економічної шкоди Сенті. Хоча не всі учасники приписали вибухи, пов'язані з мінами, діям Бастана, Службі безпеки Сенти буде доручено розслідувати міни/мінування як терористичну атаку і провести антитерористичні операції в околицях морського порту «Південний». Паралельно Міністерство закордонних справ попросить НАТО направити в цей район оперативну групу по боротьбі з мінами. Проте, учасники не уточнили структуру командування та управління силами НАТО у ВЕЗ Сенти, а також не були роз'яснені вимоги до співпраці/координації між силами НАТО і Службою безпеки, що проводить антитерористичні операції в тому ж районі.

Прагнучи бути менш реактивними і такими, що реагують на обставини, Синдикат визнав, що дії Бастана можуть мати колективну мету – створити оперативне середовище для проведення Бастаном набагато більш масштабної операції. Як результат Синдикат запропонував Раді національної безпеки і оборони доручити морським службам (у тому числі Військово-Морським силам): забезпечити безпеку судноплавства, збільшити військову присутність на прибережних територіях і острові Тотара. Водночас як і протягом усього навчання, члени Синдикату вважали, що тристоронній підхід, що включає оборонну військову стратегію, зосередження уваги на деескалації та міжнародна дипломатія, виявиться ефективним. Кожного разу, коли ситуація змінювалася, учасники обговорювали та визначали ролі та повноваження кожного департаменту/відомства Сенти.

На цьому етапі навчань учасники домовилися, що Президент Сенти збере РНБО, аби запропонувати введення воєнного стану в постраждалому регіоні. Учасники мали різні переконання щодо того, як воєнний стан вплине (відобразиться) на дії та/або цілі Бастана. Воєнний стан було сприйнято багатьма як ще один приклад оборонної військової стратегії. Таким чином, в учасників були різні погляди на те, як можна використовувати воєнний стан для планування/координації наступальних операцій або які умови повинні бути виконані та ким (наприклад, силами Бастана, Військово-Морськими силами Сенти тощо), аби скасувати воєнний стан.

Відна 3.3.1: День 53: 27 лютого, 11:00

Два вибухи потопили два вантажних судна, які належать Сенті та Зестану, що слідували в морський порт «Південний». Дві плавучі контактні міни часів Другої світової війни виявлені літаками-розвідниками та знищені Військово-Морськими силами Сенти. Уряд Зестана публікує початкові технічні докази, що компрометують припущення про старі контактні міни: всі пошкодження розташовані глибше під корпусом, поруч з кормою, а всі вибухи відбулися в машинному відділенні. Деякі міжнародні судноплавні компанії оголошують ВЕЗ Сенти небезпечною для судноплавства.

Реагування на Відну 3.3.1

Члени Синдикату одностайно погодилися з тим, що дії Бастана ілюструють очевидну мету завдати економічної шкоди Сенті. Хоча не всі учасники приписали вибухи, пов'язані з мінами, діям Бастана, Службі безпеки Сенти буде доручено розслідувати міни/мінування як терористичну атаку і провести антитерористичні операції в околицях морського порту «Південний». Паралельно Міністерство закордонних справ попросить НАТО направити в цей район оперативну групу з розмінування. Проте, учасники не уточнили структуру командування та управління силами НАТО у ВЕЗ Сенти, а також не були роз'яснені вимоги до співпраці/координації між силами НАТО і Службою безпеки, що проводить антитерористичні операції в тому ж районі.

Відна 3.3.2: День 54: 28 лютого, 09:00

Військово-морські сили Бастана оголошують район стрільби і навчань небезпечним і блокують морський шлях в Одеський морський порт. Інтенсивні військові навчання, в тому числі з використанням різних систем озброєння, тривають вже два тижні та проводяться в безпосередній близькості до торгових суден, які проходять через цей район, що порушує судноплавство.

Реагування на Відну 3.3.2

Прагнучи бути менш реактивним і такими, що реагують на обставини, Синдикат визнав, що дії Бастана можуть мати колективну мету - створити оперативне середовище для проведення Бастаном набагато більш масштабної операції. Як результат Синдикат запропонував Раді національної безпеки доручити морським службам (у тому числі Військово-Морським силам): забезпечити безпеку судноплавства, збільшити військову присутність на прибережних територіях і острові Тотара. Водночас як і протягом усього навчання, члени Синдикату вважали, що тристоронній підхід, що включає оборонну військову стратегію, зосередження уваги на деескалації та міжнародна дипломатія, виявиться ефективним. Не було вказано поетапного плану дій щодо того, які департаменти/відомства/Збройні Сили Сенти будуть керувати підходом і як паралельно (або послідовно) будуть координуватися зусилля між зацікавленими сторонами.

Ввідна 3.3.3: День 55: 1 березня, 12:00

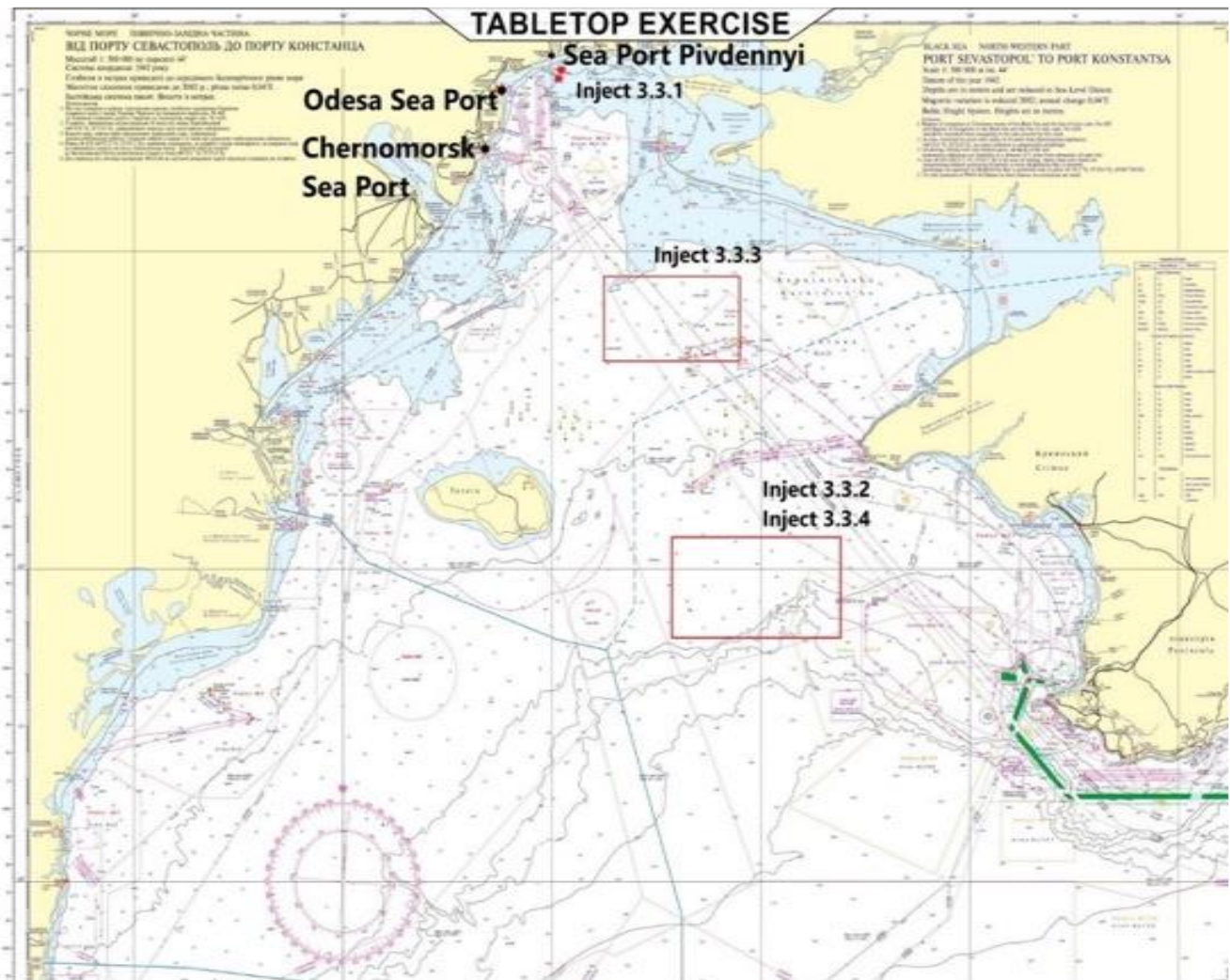
Бастан встановлює зону контролю у ВЕЗ Сенти, де кораблі, що прямують у Сенту, зупиняються й обшукуються військово-морськими силами Бастана, береговою охороною або і тими, і тими. Мотивацією таких дій, як оголосив Бастан, є підозрювана терористична загроза невизначеним стратегічним цілям. Кораблі піддаються вибірковому контролю. Затримки варіюються від п'яти годин до двох днів. Середній час очікування одного корабля становить 20 годин.

Реагування на Ввідну 3.3.3

Синдикат не надав чіткої відповіді на цю ввідну.

Ввідна 3.3.4: День 55: 1 березня, 16:00

ВМС Бастана розширюють територію навчань й оголошують значну частину ВЕЗ Сенти небезпечною. Масштабні військові навчання перешкоджають доступу до більшості портів Сенти в морі Нуар. В результаті цього великі поромні та судноплавні компанії зупиняють надання своїх послуг, а деякі компанії припиняють свою діяльність. Поромне сполучення зі Зестаном припинене.



Реагування на Ввідну 3.3.4

На цьому етапі навчань учасники домовилися, що Президент Сенти збере РНБО, аби запропонувати введення воєнного стану в постраждалому регіоні. Учасники мали різні переконання щодо того, як воєнний стан вплине (відобразиться) на дії та/або цілі Бастана. Воєнний стан було сприйнято багатьма як ще один приклад оборонної військової стратегії. Таким чином, учасники не обговорювали те, як можна використовувати воєнний стан для планування/координації наступальних операцій або які умови повинні бути виконані та ким (наприклад, силами Бастана, Військово-Морськими силами Сенти тощо), аби скасувати воєнний стан.

5.4. Епізод 4: Гібридна війна

Напруженість у відносинах між Бастаном і Сентою досягла найвищого рівня за всю їх історію. Військова розвідка Сенти повідомила про безпрецедентне нарощування військових сил і засобів на базах Бастанського флоту в морі Нуар. На острові Тотара почала відбуватися значна кількість провокаційних нещасних випадків. Повідомлення про втрату сигналів GPS і GSM на острові. Підключення до Інтернету на острові зникло.

У той самий час Сента продовжує стикатися зі збільшенням кількості кібератак на урядові та місцеві установи та постачальників критично важливих послуг. ЗМІ Бастана і Сенти повідомляють в агресивній манері про нездатність центральної та місцевої влади Сенти надавати населенню критично важливі послуги. Більш того, вищі командири Збройних сил Сенти в Києві та посадові особи Військово-морських сил в Одесі та на острові Тотара отримали електронні листи з непідтверджених профілів з прямим попередженням «не виконувати накази політичного керівництва Сенти, інакше вони та їхні сім'ї будуть в небезпеці».

Соціальні мережі сповнені повідомлень і активних дискусій про можливе відділення південної частини Сенти. Ті ж новини поширюються через офіційні вебсторінки регіональних рад. Все вищевказане призводить до тиску та напруження всередині державних установ, правоохоронних органів і збройних сил. За останні 24 години різко посилюються вуличні демонстрації проти уряду Сенти, а саме в центральних містах південних регіонів: Одесі, Миколаєві та Херсоні. В результаті уряд функціонує на межі можливого, а населення збентежене.

На тлі значних кібератак, психологічного тиску, поширення дезінформації і дедалі більших вуличних протестів у південних регіонах на острові Тотара раптово висадилася значна кількість о/с збройних сил без розпізнавальних знаків. Доступ до порту острова Тотара заблокований вантажними суднами без розпізнавальних знаків і прапора держави. Доступ по воді до острова Тотара відрізаний. Бурові установки для видобутку вуглеводнів на острові Тотара, розташовані у ВЕЗ Сента, були захоплені й тепер знаходяться під повним контролем озброєних людей без розпізнавальних знаків.

Реагування на Епізод 4

Члени Синдикату погодилися, що, оскільки в озброєних людей не було розпізнавальних знаків, Сента визнаватиме їх як терористів. Як результат цього буде проводитися антитерористична операція в умовах воєнного стану для усунення озброєних людей. У цій ситуації Синдикат роз'яснив, що антитерористична операція повинна координуватися Службою безпеки.

Після трьох послідовних ввідних, які включали наступальні операції, що проводяться озброєними людьми без розпізнавальних знаків, учасники були (але не точно) внутрішньо (всередині Сенти)

зосереджені на захисті критичної інфраструктури та перекиданні додаткових сил на острів Тотара. В результаті в обговореннях менше згадувалися Міністерство закордонних справ та інші невійськові відомства/департаменти як співучасники та інструменти для всього урядового підходу щодо досягнення спільної мети (наприклад, арешт озброєних людей, відновлення доступу до Південно-Західного штабу Військово-Морських сил тощо). Аналогічним чином, учасники обговорили цінність і ймовірність отримання міжнародної підтримки (в тому числі від НАТО). В результаті цього деякі учасники все частіше пропонували розв'язати та усунути загрозу, що надходить від озброєних людей, через антитерористичні/військові операції, на відміну від зміцнення Міжвідомчої та військово-цивільної співпраці для протидії гібридним загрозам.

Ввідна 4.3.1: День 56: 2 березня, 05:00

Озброєні люди без розпізнавальних знаків захопили вісім газових вишок біля острова Тотара у ВЕЗ Сенти. Вони десантувалися на вишки за допомогою вертольотів і захопили їх. Військово-морські сили Бастана встановлюють зону контролю навколо бурових установок, а саме в районах Штурмівського і Голіцинського газових родовищ. Цивільні судна й літаки повідомляють про значний збій у роботі GPS-сигналів в районі моря Нуар.

Реагування на Ввідну 4.3.1

Члени Синдикату погодилися, що, оскільки в озброєних людей не було розпізнавальних знаків, Сента визнаватиме їх як терористів. Як результат цього буде проводитися антитерористична операція в умовах воєнного стану для усунення озброєних людей. Додатково не були визначені керівна військова служба та/або координація, необхідні для проведення операції.

Ввідна 4.3.2: День 58: 4 березня, 02:00

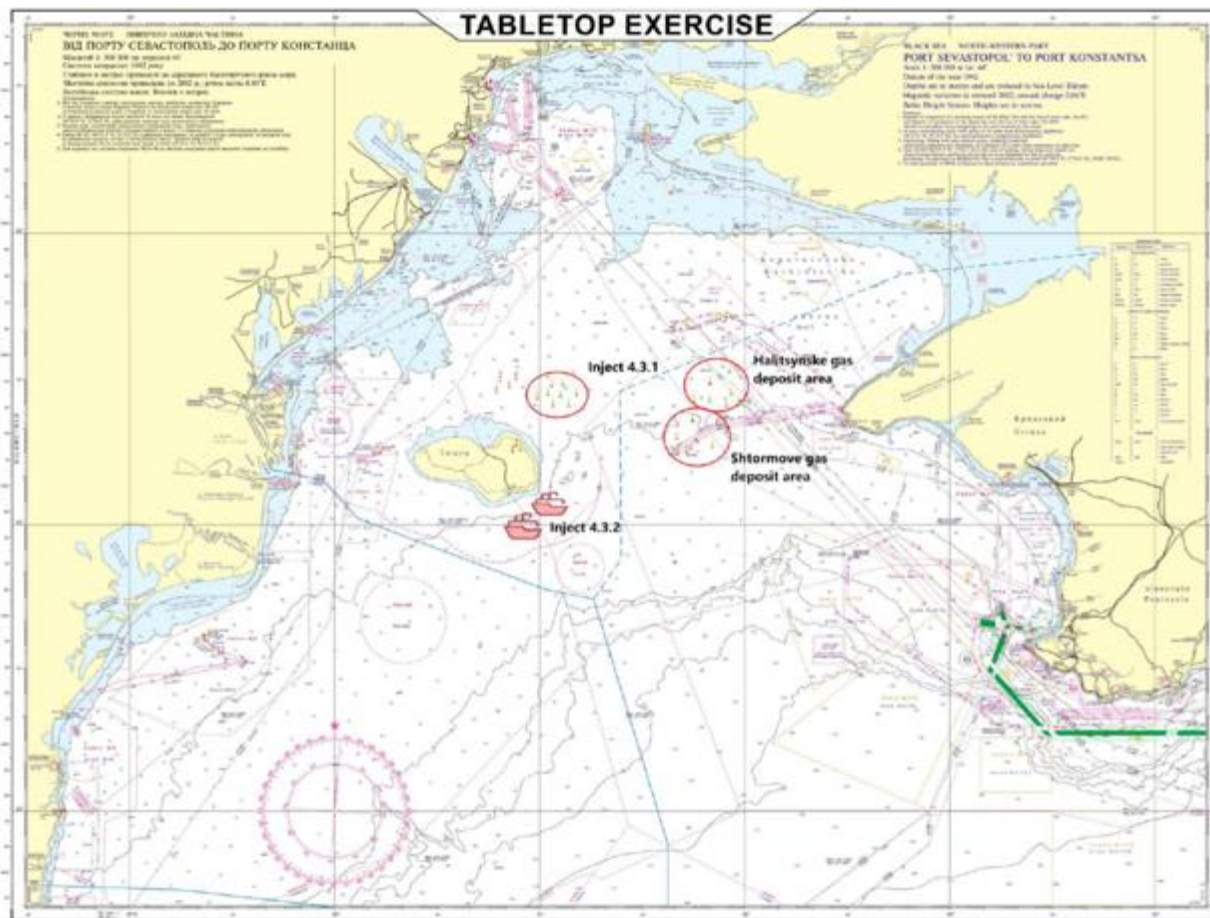
З моменту встановлення зони контролю у ВЕЗ Сенти контроль над морськими комунікаціями з боку Бастана триває. Значна кількість добре озброєних людей без розпізнавальних знаків і пробастанських активістів десантуються на острів Тотара вночі за допомогою вертольотів і цивільних вантажних суден. Повідомлення про захоплення місцевих установ і основної військово-морської бази Сенти на острові. Для повного блокування доступу до військово-морської бази використовуються вантажні судна без розпізнавальних знаків і прапорів держави.

Реагування на Ввідну 4.3.2

Члени Синдикату шукали дипломатичні засоби для припинення криз, але тим часом економічна ситуація в Сенті продовжувала погіршуватися через збій в роботі портів, морських перевезень, диверсії тощо. В першу чергу через залежність членів Синдикату від дипломатії та підтримки з боку членів НАТО і країн-партнерів, масштаби перспективної військової операції продовжували збільшуватися (для усунення сил Бастана і неідентифікованих з території Сенти [в тому числі ВЕЗ]), криза продовжувала загострюватися, а стійкість критичної інфраструктури Сенти та готовність до (додаткових) гібридних загроз продовжували знижуватися.

Ввідна 4.3.3: День 58: 4 березня, 13:00

Військові кораблі Військово-Морських сил Сенти, розташовані в районі порту Тотара, заблоковані та захоплені озброєними людьми без розпізнавальних знаків. Повідомляється про декількох постраждалих. Центральний уряд і військова влада Сенти повністю втрачають доступ до свого Південно-Західного штабу Військово-Морських сил, що розташований на острові Тотара. Зв'язок з ВЕЗ сусідніх держав перервано.



Реагування на Ввідну 4.3.3

Після трьох послідовних ввідних, які включали наступальні операції, що проводяться озброєними людьми без розпізнавальних знаків, учасники були (але не точно) внутрішньо (всередині Сенти) зосереджені на захисті критичної інфраструктури та перекиданні додаткових сил на острів Тотара. В результаті в обговореннях менше згадувалися Міністерство закордонних справ та інші невійськові відомства/департаменти як співучасники та інструменти для всього урядового підходу щодо досягнення спільної мети (наприклад, арешт озброєних людей, відновлення доступу до Південно-Західного штабу Військово-Морських сил тощо). Аналогічним чином, учасники обговорили цінність і ймовірність отримання міжнародної підтримки (в тому числі від НАТО). В результаті цього учасники все частіше пропонували розв'язати та усунути загрозу, що надходить від озброєних людей, через антитерористичні/військові операції, на відміну від зміцнення Міжвідомчої та військово-цивільної співпраці для протидії гібридним загрозам.

5.5. Епізод 5: Посткризова стабілізація

Цей епізод присвячений посткризовому відновленню та процесу стабілізації. Посткризова стабілізація відбувається після закінчення кризового сценарію – з 7 березня 20XX року. Також потрібно обговорити питання управління в кризових ситуаціях.

Кожному синдикату буде запропоновано кілька питань для обговорення посткризової стабілізації.

1. Чи є законодавство про безпеку на морі вичерпне (достатнє) на сьогодні? Якщо ні, то які пріоритетні області для його поліпшення в посткризовому аналізі?

Відповідь

Учасники обговорили необхідність розробки та прийняття Стратегії морської безпеки країни, завершення законодавчої роботи з демаркації морських кордонів країни за участю міжнародних механізмів, а також внесення змін до чинного законодавства та розробки нового законодавства для забезпечення захисту національних інтересів на морі. Учасники також запропонували розробити та впровадити спільну стратегію безпеки на морі з НАТО і країнами-партнерами в Азово-Чорноморському регіоні.

2. Які проблеми із налагодженням належної (безперервної) взаємодії компонентів сектору безпеки та оборони та цивільного компонента (Державна прикордонна служба, Військово-морські сили, Державна служба з надзвичайних ситуацій, Адміністрація морських портів і керівництво портів, Державна служба з безпеки на транспорті, Морська пошуково-рятувальна служба, Державне агентство рибного господарства, Державна екологічна інспекція) для забезпечення посткризової безпеки на морі?

Відповідь

На початку навчань декілька членів Синдикату були чітко переконані в належній взаємодії компонентів сектору безпеки та оборони, а цивільний компонент працює безперебійно в докризовому і посткризовому середовищі морської безпеки. Однак у міру проходження навчань кілька учасників висловили протилежні думки про взаємодію між зацікавленими сторонами, особливо щодо ролей та обов'язків у секторі безпеки та оборони. Оскільки члени Синдикату склалися переважно з військових, то вони часто приділяли особливу увагу взаємодії компонентів сектора безпеки й оборони. Зокрема, члени Синдикату не змогли колективно домовитися про ролі та обов'язки щодо взаємодії незалежно від законодавства/законів. Рухаючись вперед, члени Синдикату визнали користь подальшого вивчення взаємодії також і між цивільними компонентами (для забезпечення посткризової безпеки на морі).

3. Які проблеми взаємодії державного та приватного секторів у сфері морської безпеки? Які варіанти врегулювання?

Відповідь

Знову ж таки, через обмежене представництво серед членів Синдикату фахівців з досвідом роботи в приватному секторі часто виникали проблеми, пов'язані із взаємодією державного і приватного секторів. Оскільки члени Синдикату часто посилалися на важливість морського сектора для економіки Сенти, то багато членів синдикату визнали необхідність розширення взаємодії державного і приватного секторів у сфері морської безпеки. Крім того, департаментам/відомствам Сенти було б корисно пройти навчання з питань сприйняття приватним сектором морської безпеки та її важливості для галузі.

5.6. Ключові висновки

Вимога введення воєнного стану в умовах гібридної загрози. Оголошення воєнного стану обговорювалося Синдикатом на основі окремих гібридних дій і апогею безлічі гібридних дій.

Рекомендація: Визначити ознаки гібридних загроз, які кожна окремо або разом призведуть до оголошення воєнного стану. Прийняти законодавство в міру розвитку гібридних загроз. Постійний моніторинг і виявлення нових показників невійськових загроз, що зачіпають морські інтереси країни. Визначити порядок дій сектору оборони та безпеки на основі цих загроз. Розробити нові способи застосування аспектів воєнного стану в умовах гібридної загрози без необхідності оголошення воєнного стану, такі як підвищення рівня антитерористичної загрози та використання антитерористичних операцій як протидії.

Тривала обстановка гібридних загроз. Члени Синдикату шукали дипломатичні засоби для припинення криз, але тим часом економічна ситуація продовжувала погіршуватися через зриви в роботі портів, морських перевезень, диверсії тощо. **Рекомендація:** Беручи до уваги нову концепцію забезпечення національної системи стійкості, в документах конкретних установ повинна бути уточнена процедура, а також забезпечене здійснення заходів реагування на кризові ситуації. Зокрема, включити політичні, інформаційні, економічні, соціально-гуманітарні, військові та інші заходи з мінімізації загроз, впливу і наслідків гібридних дій.

Визначення гібридних загроз як засіб зменшення наслідків гібридних дій. Протягом усього навчання члени Синдикату часто мали труднощі з визначенням застосовних законів у сфері морського права та відповідного міністерства, яке забезпечує їх дотримання, адже ґрунтувалися на неоднозначних визначеннях різних гібридних загроз. **Рекомендація:** Виявлені показники гібридної загрози повинні бути приведені у відповідність з показниками, які використовуються в країнах-членах НАТО та враховані у відповідних планах, регламентах і процедурах реагування на кризові ситуації, аби усунути неоднозначність у розумінні між національними міністерствами та членами НАТО.

Оборонні спроможності та потенціал членів НАТО, країн-партнерів і міжнародних організацій. Коли політичне та/або військове керівництво вирішило, що для посилення Збройних сил та/або заповнення прогалин у спроможностях потрібні додаткові оборонні спроможності та можливості, члени Синдикату вміло залучали членів НАТО, країни-партнери та/або міжнародні організації. **Рекомендація:** При підготовці до координації дій між Збройними Силами України та членами НАТО, країнами-партнерами і міжнародними організаціями Україні слід виявити прогалини в спроможностях з урахуванням нових змін у загрозах критичній інфраструктурі та ланцюжках постачання і включити зацікавлені сторони в національне управління кризами. Водночас передбачити спрощення механізмів залучення іноземних підрозділів, коштів та ресурсів.

Розуміння внутрішнього та міжнародного морського законодавства для протидії гібридним загрозам. Протягом усього навчання супротивник використовував міжнародні та внутрішні закони для виправдання та/або посилення гібридної загрози з боку своїх сил, що діяли у виключній економічній зоні України. В Україні уряд цивільних міністрів має оперативний контроль над Збройними Силами для ведення конвенційних бойових дій. А уряд противника, очолюваний цивільними особами, має оперативний контроль над збройними силами для проведення гібридних дій і конвенційних бойових дій. В результаті Збройні сили кожної країни діють по-різному щодо того, як вони використовують плани, регламенти та процедури. **Рекомендація:** Планування і реалізація

заходів морської безпеки повинні здійснюватися з урахуванням прогнозу дій противника на основі його чинного законодавства і можливого зловживання або нехтування міжнародним правом.

Вимога до загальної оперативної картини із запізненням у часі. З метою підвищення стійкості критичної інфраструктури та готовності до гібридних загроз всі зацікавлені сторони, ймовірно, зроблять свій внесок у загальну оперативну картину морської безпеки. **Рекомендація:** Підвищити рівень обізнаності про морську обстановку, скоротити час прийняття рішень щодо реагування на гібридні загрози на морі, удосконалити міжвідомчі процедури збору, обробки та узагальнення інформації, а також передбачити створення національного координаційного центру морської безпеки. Забезпечити залучення іноземного персоналу до роботи центру для підвищення рівня оперативної сумісності з країнами-членами НАТО

Багатосферний підхід до підвищення ефективності збору інформації, спостереження та розвідки (ISR) проти гібридних загроз. Синдикат обговорив необхідність створення багатосферної інтегрованої системи ведення розвідки (ISR) для протидії гібридним загрозам. **Рекомендація:** Забезпечити участь всіх компонентів сил безпеки і оборони, цивільних організацій та установ, які виконують завдання в морській сфері (на морі), в інтересах охоплення надводного і підводного середовища та обміну інформацією в цій галузі. Для цього необхідно створити державну інтегровану систему ведення розвідки у водах морів і басейнах річок.

Стратегія Збройних Сил в нестандартній обстановці. **Рекомендація:** Під час планування антикризового реагування забезпечити необхідні спроможності для захисту національних інтересів, у тому числі економічних, політичних та інших, їх підтримки та використання відповідно до встановлених рівнів готовності.

6. Синдикат 4: СТРАТКОМ

6.1. Епізод 1: Доконфліктна фаза: Гібридний вплив

Посилюється політичне та економічне залякування з боку влади Бастана. На підставі угоди про транзит газу, яка була підписана між Бастаном і Сентою минулого року, уряд Бастана звинуватив Сенту в порушенні положень угоди. Сента заперечує будь-які порушення. Однак ЗМІ Бастана і деякі ЗМІ Сенти, контрольовані Бастаном, продовжують поширювати повідомлення про порушення Сенти, підкреслюючи важливість відповідної угоди для енергетичної безпеки Європи, оскільки транзит газу в європейські країни частково забезпечується через територію Сенти.

Ситуацію ускладнює той факт, що між Бастаном і Велою не укладено новий контракт на постачання газу. Враховуючи суперечки щодо договірних положень, Бастан тимчасово істотно скорочує постачання газу в Велу. Вела максимально відбирає газ з транзитного трубопроводу, обмежуючи постачання газу споживачам Сенти в Одеській області, недалеко від кордону з Румунією.

Тим часом Бастан ввів обмеження на імпорт сільськогосподарських, промислових товарів і металевих виробів, палива, хімікатів і нафтопродуктів із Сенти. Крім того, Бастан припиняє постачати нафтопродукти в Сенту автомобільним, залізничним транспортом і трубопроводами.

В Інтернеті були виявлені три вебсайти з ідентичним візуальним оформленням і функціями офіційних вебсайтів Оператора ГТС Сенти, Оператора PSG і компанії «Нафтогаз». Крім того, на електронні адреси регіональних урядових установ Сенти були надіслані листи з фішинговими функціями та прикріплені текстові документи Microsoft Word.

У ЗМІ з'явилися повідомлення про потужну кібератаку на внутрішню мережу Liebherr в Німеччині. В результаті портові крани в морському порту Поті в Зестані перестали працювати.

З середини грудня берегова охорона Сенти регулярно повідомляє про присутність Військово-морських сил Бастана у ВЕЗ Сенти. Повідомляється, що Бастан проводив військові навчання в морі Нуар у безпосередній близькості від фарватерного проходу торгових і пасажирських суден з/в порти Одеської області.



Синдикат стратегічних комунікацій обговорює форми реагування на ввідні по сценарію в рамках КШН НАТО «НЕПОРУШНА СТІЙКІСТЬ 20» в Одесі, Україна.

Ввідна 1.4.1: День 1: 6 січня, 11:00

Через рік після підписання угоди про транзит газу влада Бастана звинувачує Сенту в порушенні угоди, попереджаючи про розірвання контракту і припинення постачання газу через територію Сенти. ЗМІ Бастана посилюють трансляцію повідомлень про порушення Сентою Угоди про транзит газу, які базуються на наративі про те, що Сента може тримати в заручниках не тільки своє населення, а і європейські країни. Ця інформація також транслюється деякими телевізійними каналами новин у країнах ЄС.

Реагування на Ввідну 1.4.1

Учасники сперечалися про те, яке повідомлення слід сформувати у відповідь і як це зробити. Чи існує криза на цій фазі та чи повинні вони ставитися до цього як до кризи? Боротьба з фейковим наративом, який транслюють ЗМІ Бастана, була їх пріоритетом, а саме через дипломатичні канали та засоби масової інформації. Однак загалом було визнано, що не існує чіткого регламенту щодо того, яке відомство має бути провідним у досягненні цієї мети щодо протидії наративу, а це призводить до невизначеності щодо того, яким насправді має бути повідомлення. Оскільки в Сенті відсутній чіткий процес створення групи реагування на кризу, також було багато дискусій про те, хто приймає рішення про наявність кризи, а потім створює спеціальну групу реагування на кризу. У певний момент багато учасників зациклилися на виробленні принципів і підходів і не мислили стратегічно. Лідери нагадали учасникам, що це лише частина гібридних дій Бастана, і що наратив, спрямований на те, аби Сента виглядала ненадійною як транзитна країна, був лише початком. Учасники знали, що робити, але не було згоди щодо того, як це зробити. Це сприяло усвідомленню того, що Сенті необхідне агентство СТРАТКОМ на рівні уряду, аби його повідомлення на протидію наративам Бастана були чіткими, несуперечливими та показували загальну картину.

Ввідна 1.4.2: День 14: 19 січня, 02:00

Бастан в соціальних мережах активно обговорює, що запідозрені кібератаки, які призвели до збоїв в роботі найбільших банків Сенти (ПриватБанк, Ощадбанк), а раніше центральних державних установ, були спрямовані на прикриття відмивання грошей корумпованим урядом і бізнесом.

Реагування на Ввідну 1.4.2

Тут на перший план вийшли представники відповідних відомств, аби спростувати цю неправдиву інформацію. Дискусія була зосереджена навколо заяви банків про розкриття інформації про кібератаки, а також про необхідність створення інформаційної переваги та здатності ефективно інформувати суспільство. Спростування цих неправдивих наративів перебувало, як здавалося, в центрі уваги з розмовами про залучення громадських організацій до спростування фейків (серія публікацій), проведення круглих столів. Крім того, Синдикат визначив Раду національної безпеки і оборони як провідну установу, яка повинна визначити рівень загрози та направляти інформацію у відповідні відомства. Вони вирішили, що поліція повинна виступити із заявою про розслідування інформації про кібератаки. Знову ж таки, проблема полягала не в обміні повідомленнями, а в тому, як донести повідомлення до різних аудиторій, яким необхідно почути про протидію цим сфабрикованим наративам Бастана.

Ввідна 1.4.3: День 16: 21 січня, 11:00

Багато клієнтів постять багато повідомлень в соціальних мережах про неправильну роботу Розрахункових і білінгових центрів у сфері комунальних послуг, багатьом обуреним споживачам помилково нараховують заборгованість.

Реагування на Ввідну 1.4.3

Учасники підкреслили необхідність рішучих дій уряду, аби допомогти зменшити рівень паніки з приводу фейкових історій про виставлення рахунків за комунальні послуги. РНБО і МВС кілька разів вказувалися як відомства, які повинні реагувати й займатися цими наративами та протидією їм. Крім того, прозвучала пропозиція про створення спеціального агентства, а інші наполягали на тому, що необхідно створити центр СТРАТКОМ на рівні уряду, який координував би комунікації між відповідними відомствами на національному, регіональному та місцевому рівнях. Також говорилося про те, аби оцінити серйозність цієї загрози, а потім попросити лідерів думок з приватного сектора допомогти зі спростуванням наративу про аномалії з виставленням рахунків. Тут нема потреби в допомозі з боку міжнародної спільноти, а наратив має виходити від національної влади Сенти, оскільки існували побоювання, що опора на іноземних експертів або їх допомога сприятиме наративу Бастана. Знову ж таки, проблема тут полягала в тому, як надсилати повідомлення та як орієнтуватися на відповідну аудиторію, а не на саме повідомлення. Синдикат стикнувся з постійною відсутністю чіткого розуміння того, хто несе відповідальність за керівництво і координацію заходів з реагування на кризові ситуації, а отже, хто повинен координувати інформаційне реагування між різними залученими міністерствами та відомствами.

Ввідна 1.4.4: День 21: 26 січня, 06:00

По поштових скриньках людей в Одесі та інших містах області поширюється значна кількість листівок і флаєрів із закликом до людей повстати проти корумпованих місцевих органів влади.



Реагування на Ввідну 1.4.4

СБУ відстежує і виявляє загрози. Було визнано, що все це необхідно для того, аби вони могли створити хороший контраргумент. Потім було запропоновано, аби СБУ та обласна державна адміністрація стежили за ситуацією в регіоні, при цьому ОДА відстежувала мітинги та основні неправдиві повідомлення, що поширюються, а СБУ виявляла загрозу та постійно інформувала внутрішню аудиторію про ситуацію. Рекомендується використовувати телефонні гарячі лінії, соціальні мережі та компанії мобільного зв'язку, аби забезпечити охоплення якомога більше людей власними повідомленнями. Зрештою, потреба в Національному координаційному центрі СТРАТКОМ знову стала очевидною, як і необхідність піклуватися не тільки про внутрішню аудиторію, але й про вплив на іноземних союзників і партнерів, а також на ворожу аудиторію.

6.2. Епізод 2: Гібридні операції низької інтенсивності

На початку лютого погодні умови в південних районах Сенти погіршилися. Швидкість вітру досягає 50 м/с, що завдає значної шкоди, зокрема, в Одеській області.

Введені Бастаном обмеження на імпорт товарів сільського господарства, обробної промисловості та металевих виробів, палива, хімікатів і нафтопродуктів із Сенти сприяють занепаду економіки

Сенти, яка вже знаходиться в стані рецесії. Пробастанські активісти використовують економічний спад як шанс посилити протести проти уряду Сенти. Соціальна напруженість досягла свого піка, коли в Інтернеті поширилася новина про рішення Одеської міської ради про вихід Одеської області зі складу Сенти.

Діяльність пробастанських активістів та інцидентами у сфері кібербезпеки постійно порушують роботу Одеського морського порту. Крім того, цивільні судна і кораблі берегової охорони Сенти повідомляли про технічні неполадки у роботі своїх навігаційних систем.

Крім того, судна Бастана діють агресивно проти риболовецьких суден Сенти. Кораблі берегової охорони Бастана залякують і погрожують вантажним суднам Сенти, а також суднам іноземних держав. Нещодавно Військово-морські сили Бастана надали підтримку незаконній діяльності з розвідки газу та встановлення бурових установок на території ВЕЗ Сенти. Навколо бурових установок був встановлений цілодобовий охоронний патруль Військово-морських сил Бастана.

Ввідна 2.4.1: День 22: 27 січня, 08:00

Під приводом погіршення економічної ситуації та зростання цін на нафтопродукти й пальне пробастанські активісти починають блокувати основні дороги, портові об'єкти та паливні термінали в Одесі. ЗМІ Бастана звинувачують правоохоронні органи Сенти в застосуванні сили та вбивстві десятків протестувальників.

Реагування на Ввідну 2.4.1

Брехливі наративи Бастана посилюються, а ЗМІ Бастана оголошують, що поліція Сенти вбиває протестувальників в Одеській області. Синдикат погоджується з тим, що це національна, а не тільки регіональна проблема, і що реакція та обмін повідомленнями повинні координуватися на національному та регіональному рівнях. Розмови про створення Національного центру СТРАТКОМ тривають, з чіткішими ідеями щодо структури цього відомства. Була запропонована мобілізація журналістів, лідерів громадської думки та Міністерства закордонних справ як головних учасників цього процесу, хоча процес мобілізації та координації цих учасників так чітко не обговорювався. Також пропонувалося, аби СБУ заблокувала соціальні мережі Бастана, а потім поширила правдиву інформацію, але процес і законність цих пропозицій зіткнулися з протидією.

Ввідна 2.4.2: День 24: 29 січня, 12:00

На сайті Одеської міської ради йдеться про те, що обласна влада вирішила проголосити незалежність від Сенти та стати Одеською Автономною Республікою. Звернення за допомогою до влади Бастана.

Реагування на Ввідну 2.4.2

Учасники визнали, що цей фейковий наратив буде легко розвінчати, і було висловлено припущення про те, що СБУ буде головним органом, який виступатиме проти цього наративу. Було не досить зрозуміло, як цього ефективно досягнути. Експерти також запропонували, як боротися з цими зростаючими кампаніями дезінформації, які проводить Бастан, нагадавши їм про необхідність мислити стратегічно. Експерти також закликали їх подумати про те, аби донести інформацію до трьох аудиторій: заспокоїти внутрішню аудиторію, продемонструвати рішучість міжнародній спільноті та завадити наративам Бастана. До цього моменту Синдикат думав про перші дві аудиторії, але не про третю. Синдикат мав хороші ідеї щодо того, що робити, але вони вимагали більше структури та керівництва, аби бути більш ефективними для СТРАТКОМ.

Відна 2.4.3: День 40: 14 лютого, 20:00

У засобах масової інформації та в соціальних мережах наявна інформація про загальнодоступність інформації про виставлення рахунків за комунальні послуги із зазначенням особистих даних клієнтів (таких як ім'я, адреса, номер телефону, адреса електронної пошти).

Реагування на Ввідну 2.4.3

Все ще пам'ятаючи пропозиції експертів для попередньої ввідної, члени Синдикату зосередилися на необхідності швидкого визначення правдивості цієї історії, оскільки люди можуть запанікувати, якщо їх особиста інформація була зламана хакерами. Правдива інформація повинна бути опублікована негайно та часто оновлюватися, аби випереджати кампанію дезінформації Бастана. Тут головним пріоритетом стає внутрішня аудиторія. Криза вже відбувається в інших сферах, тому СТРАТКОМ повинен подумати про можливі наступні кроки інформаційних операторів Бастана. Синдикат також визначив, що відсутність електроенергії, опалення та їжі, ймовірно, була більш нагальною проблемою для їх внутрішньої аудиторії.

Відна 2.4.4: День 43: 17 лютого, 10:00

Танкер, що належить Сенти, раптово втрачає управління і стикається з вантажним судном Бастана у ВЕЗ Сенти, що призводить до витоку нафти та значної пожежі. Повідомляється про декількох постраждалих. Бастан звинувачує владу Сенти в диверсії. Всі ЗМІ Бастана використовують цей приклад, аби підкреслити необхідність присутності Військово-морських сил Бастана в морі Нуар і захисту інтересів Бастана.

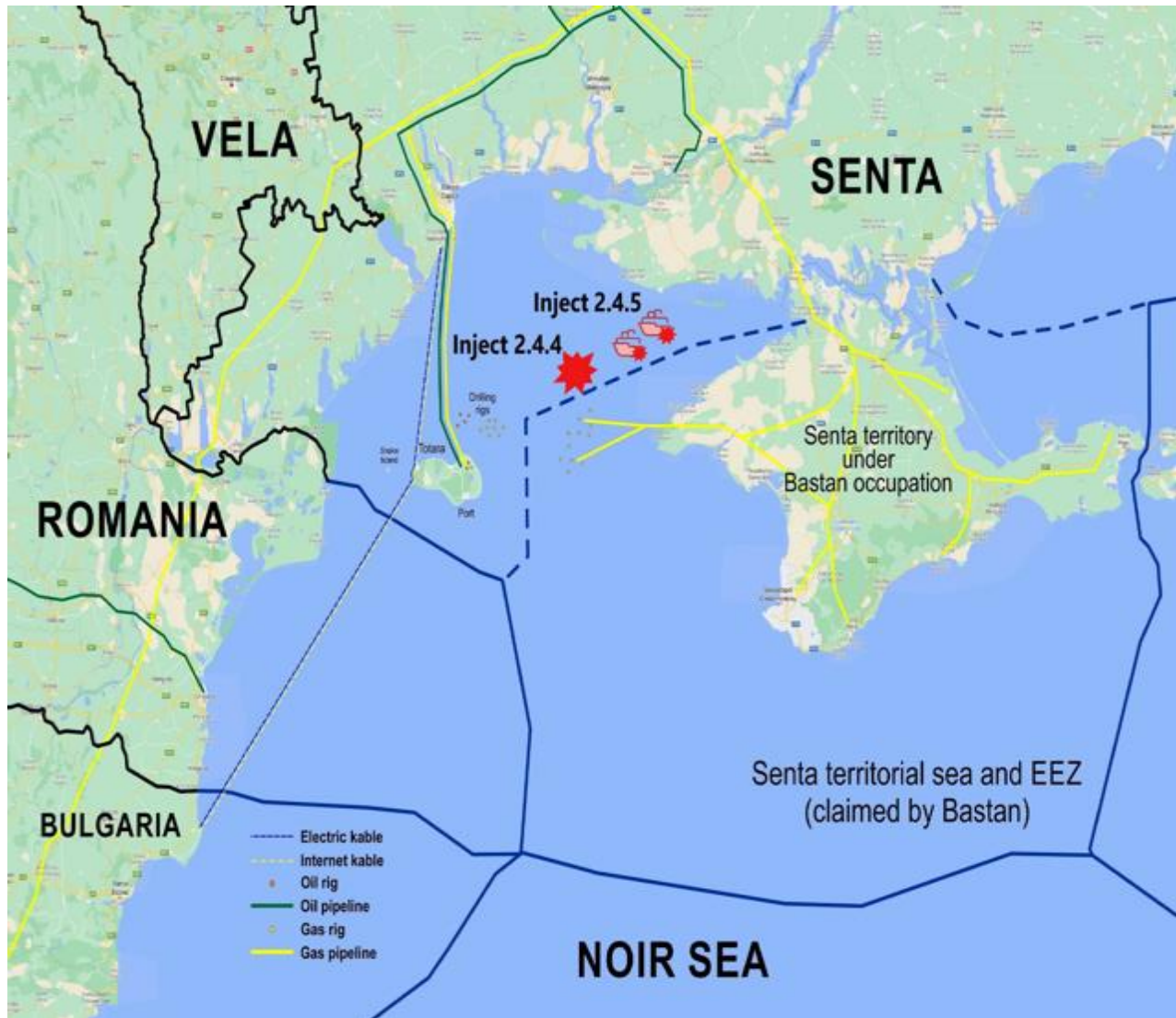
Реагування на Ввідну 2.4.4

Синдикат вирішив, що Міністерство закордонних справ і Міністерство внутрішніх справ будуть виконувати керівну роль у цій ситуації (за відсутності центру СТРАТКОМ), аби звернутися до союзників і партнерів із закликом посилити свою присутність в морі Нуар, аби гарантувати, що робота Державної служби з надзвичайних ситуацій Сенти в спірному регіоні не буде заблокована. Крім того, вони вказали на необхідність того, аби центральний уряд підтримував зв'язок і координував свої дії з місцевою владою з метою уникнення конфліктів. З'ясувати причину втрати контролю над танкером, чи було це впливом Служби безпеки Бастана, можливою кібератакою або терористичним актом, і повідомити про результати всім трьом аудиторіям. Синдикат виокремив бастанські сім'ї жертв як такі, що заслуговують на особливу увагу при складанні повідомлень міжнародній спільноті та агресору. Також було запропоновано отримати інформацію від власника судна через агентську компанію, а також від найближчих суден (Державна прикордонна служба, Військово-морські сили, Морська охорона), аби з'ясувати обставини аварії, зафіксувати перебіг події та забезпечити висвітлення в засобах масової інформації. MPRS (комунальна служба) також повинна оновлювати оперативну інформацію. Запевнити вітчизняну аудиторію, що ми знаємо про ситуацію, що ми з'ясуємо ситуацію із загиблими та надаємо допомогу всім сторонам. Також важливо надіслати повідомлення про відсутність у Сенти почуття провини. Для міжнародної аудиторії було запропоновано, аби такі провідні агентства також оперативно передавали правдиву інформацію про те, що Сента не порушувала своїх зобов'язань (на основі юридичної експертизи).

Відна 2.4.5: День 48: 22 лютого, 07:00

Військово-Морські сили Бастана і берегова охорона залякують цивільні вантажні судна Сенти та Зестану, що прямують в порти Сенти в морі Нуар, перебуваючи у ВЕЗ Сенти, і вимагають, аби вони змінили курс назад до зовнішнього кордону ВЕЗ Сенти. Згідно з даними ЗМІ Бастана, цивільний

вантажний корабель Сенти намагався навмисно врізатися в корабель ВМС Бастана. Пізніше ця інформація була повторена Міністерством оборони Бастана, яке звинувачувало кораблі Сенти в провокаційних і небезпечних діях. Згідно з повідомленнями ЗМІ Бастана, за таких обставин влада Бастана вирішила збільшити свою військово-морську присутність, аби захистити свої кораблі та інтереси від провокаційних дій Сенти.



Реагування на Ввідну 2.4.5

Тут Міністерство оборони, на думку Синдикату, має взяти на себе ініціативу, аби звернутися до партнерів Сенти та просити їх посилити свою присутність у морі Нуар. Воно також повинне оголосити про початок військових навчань. Міністерство закордонних справ має спільно з цими партнерами виступити з ініціативою про скликання засідання Ради Безпеки ООН для розгляду ситуації, що загострюється. Основною іноземною аудиторією повинні бути сусідні країни в морі Нуар, а також європейські країни з метою визначення допомоги, необхідної для врегулювання цієї кризи. Для підготовки спільних заяв Міністерство оборони та МЗС повинні активувати доступ до регіональних форматів, таких як Quadriga. Для зменшення рівня паніки серед населення слід зробити акцент на

місці події (вказати, що вона сталася не в територіальних водах Сенти). Потім Синдикат витратив значну кількість часу на обговорення процесів. Вони почали зі спроби визначити категорії криз, потім відповідний протокол дій, а потім протокол комунікацій. Експерти НАТО перенаправили їх увагу натомість не на самі визначення, а на елементи, необхідні для спільних дій, а не дій окремих осіб. Це призвело їх до висновків про необхідність централізованої структури та процесів для керівництва як кризовим реагуванням, так і процесами СТРАТКОМ.

6.3. Епізод 3: Фаза конфлікту: Гібридні операції високої інтенсивності

Критична інфраструктура Сенти піддається широкому спектру ударів кінетичною і некінетичною зброєю. Перебої в роботі газопроводу з транспортування природного газу в Південному газотранспортному коридорі позначаються на постачаннях газу в Південний регіон Сенти та сусідні іноземні держави. Більш того, існує загроза зриву опалювального сезону не лише в південній частині Сенти, але й у Харківській і Луганській областях, які, зокрема, сильно залежать від постачання газу з Бастана.

На півдні Сенти на третину збільшилася кількість надзвичайних ситуацій, пожеж і нещасних випадків, викликаних підпалами й терористичними актами з використанням вибухових речовин, що, своєю чергою, призвело до значного збільшення числа постраждалих. Є підозра про масштабний інцидент на ПАТ «Одеський припортовий завод», де повідомляється про значний викид небезпечних хімічних речовин.

Поширюється інформація про збій в роботі Південно-Сентської АЕС. ЗМІ Бастана звинувачують владу Сенти у викидах радіації. Майже одночасно поширюється інформація про атаку на гідроакумулюючу електростанцію.

Масовані кібератаки порушують роботу Одеського морського порту, в тому числі транспортування й обробку вантажів. Нападу зазнали банківські системи відділень Ощадбанку і ПриватБанку в Одеській області.

Через місяць після першої кібератаки на внутрішню мережу Liebherr в Німеччині сталася серія незначних кібератак на портові крани Liebherr по всій Європі.

У морській сфері кораблі ВМС Бастана збільшують свою присутність у ВЕЗ Сенти, використовуючи Військово-морські навчання, припиняючи міжнародні морські перевезення пасажирів і вантажів.

Ввідна 3.4.1: День 53: 27 лютого, 11:00

Два вибухи потопили два вантажних судна, які належать Сенті та Зестану, що слідували в морський порт «Південний». Дві плавучі контактні міни часів Другої світової війни виявлені літаками-розвідниками та знищені Військово-морськими силами Сенти. Уряд Зестана публікує початкові технічні докази, що компрометують припущення про старі контактні міни: всі пошкодження розташовані глибше під корпусом, поруч з кормою, а всі вибухи відбулися в машинному відділенні. Деякі міжнародні судноплавні компанії оголошують ВЕЗ Сенти небезпечною для судноплавства.

Реагування на Ввідну 3.4.1

Спочатку Синдикат запропонував розпочати визначення рівня збитку зі змінами у складі робочої групи та залученням інших відповідних відомств (ДСНС, Міністерство охорони здоров'я, Міністерство реінтеграції). Крім того, запущено постійний цілодобовий комунікаційний центр з щоденними брифінгами для українських та міжнародних журналістів. Синдикат в цілому був задоволений створенням нової спеціальної групи для боротьби з поточною кризою, тому що це їх досвід роботи з минулими кризами, але деякі члени висловили стурбованість тим, що необхідно проявляти більше передбачливості та реагувати на кризу в рамках регламентів, аби бути більш ефективним і скоротити час, необхідний для реагування. Також слід мобілізувати соціальні мережі, поширення інформації за допомогою листівок, а також громадянське суспільство в цілому. У разі надзвичайних ситуацій ДСНС повинне відігравати провідну роль у цій кризі. Альтернативні засоби комунікації, такі як мовлення на середніх хвилях і поширення листівок, повинні бути організовані до кризи. Необхідно підтримувати безперервні СТРАТКОМ з місцевим населенням, мобілізувати всі можливі засоби, демонструвати позитивний настрій і вносити пропозиції щодо того, як поліпшити економічну ситуацію. Для міжнародних партнерів Сента повинна позиціонувати себе як надійного партнера, який надає правдиву інформацію і який буде наполегливо працювати, аби якомога швидше прояснити ситуацію. Уряд повинен оголосити про тралення та безпечний прохід у районі вантажних суден та забезпечити безпеку міжнародних суден. Це повідомлення слід часто повторювати. Нарешті, дискредитації Бастана на міжнародному рівні може сприяти використання Сентою позитивних наративів.

Ввідна 3.4.2: День 54: 28 лютого, 08:00

Великі вибухи на об'єктах з виробництва та зберігання аміаку ПАТ «Одеський припортовий завод». В результаті вибуху значний викид аміаку та інших небезпечних хімічних речовин в атмосферу. Повідомляється про десятки постраждалих на заводі. Отруйна хмара аміаку рухається в бік Одеси та сусідніх міст.

Бастанські медіа та деякі ЗМІ Сенти повідомляють, що інцидент був інсценований як провокація службою безпеки Сенти.

Реагування на Ввідну 3.4.2

Синдикат вирішив створити оперативний антикризовий штаб, що складається з ДСНС+ CVS + місцевих органів влади. І знову деякі члени були стурбовані кількістю спеціальних комітетів або штаб-квартир, які створюються для розв'язання різних питань, що призводить до труднощів в ефективній координації та витрачання часу на створення груп. У новій кризовій групі повинні використовуватися комунікаційні протоколи, при цьому першочергова увага має приділятися збору інформації та інформуванню населення. Те, що це була диверсія з боку Бастана, має бути чітким сигналом. МЗС має очолити інформування зовнішньої аудиторії із залученням відповідних відомств і служб сусідніх країн (які також можуть постраждати від деяких з цих наслідків) у центральному офісі МЗС у Києві. Були запропоновані такі протоколи, як введення гарячих ліній для населення, створення мережі регіональних кризових центрів, що підпорядковані Києву, створення Центру для міжнародних журналістів у головному кризовому центрі, визначення спікерів та активація системи оповіщення про надзвичайні ситуації.

Ввідна 3.4.3: День 54: 28 лютого, 09:00

Військово-морські сили Бастана оголошують район стрільб і навчань небезпечним і блокують морський шлях в Одеський морський порт. Інтенсивні військові навчання, в тому числі з

використанням різних систем озброєння, тривають вже два тижні та проводяться в безпосередній близькості до торгових суден, які проходять через цей район, що порушує судноплавство.

Реагування на Ввідну 3.4.3

Спочатку обговорювалися наслідки: економічні втрати, втрати для міжнародного іміджу, внутрішні загрози та загроза національній безпеці, пов'язані з окупацією моря Нуар Бастаном. Потім були обговорені основні завдання та запропоновані такі підходи: якомога швидше відновлення судноплавства, консолідація міжнародної підтримки Сенти, дискредитація Бастана і його фейкових наративів, зниження соціальної напруженості в регіоні, відновлення і підтримка міжнародного іміджу Сенти, а також демонстрація підтримки міжнародної спільноти (адресована як внутрішній, так і бастанській аудиторіям), створення відчуття безпеки та довіри у населення. Механізми досягнення цих цілей в першу чергу керує Міністерство закордонних справ, оскільки необхідна активізація інформаційної та роз'яснювальної роботи з партнерами, а також консультації з Бастаном про те, що можна зробити для розрядки ситуації. Міністерство оборони також має сприяти у проведенні інформаційних операцій, інформуючи громадськість про посилення своєї присутності в регіоні. Обласна державна адміністрація має провести зустрічі з представниками бізнесу та закликати їх продовжувати виплачувати заробітну плату та дотримання стабільності цін на рівні Прем'єр-міністра.

Ввідна 3.4.4: День 55: 1 березня, 12:00

Поширюється неправдива інформація про аварійне відключення Південно-Сентської АЕС. ЗМІ Бастану звинувачують американських постачальників ядерного палива і «корумповану владу» Сенти, поширюючи повідомлення про масштабний інцидент на атомній електростанції зі значним викидом радіації. Деякі екоактивісти Сенти звинувачують владу Сенти у брехні про цей інцидент. Ґрунтуючись на інформації від Бастана, міжнародні телеканали разом з деякими ЗМІ Сенти поширюють повідомлення про можливість нового «Чорнобиля».

Реагування на Ввідну 3.4.4

Оскільки наслідки цього поширюваного наратива можуть викликати паніку в країні, навіть дестабілізацію, економічний спад, ризик появи біженців і паніку серед партнерів Сенти, головним пріоритетом має бути заспокоєння внутрішньої аудиторії. МЗС має взяти під свій контроль надання правдивої інформації про дезінформацію, демонстрацію суб'єктності Сенти, залучати американських партнерів для сприяння у проведенні роз'яснювальної роботи, а також має звернутися до міжнародних журналістів. Державна інспекція ядерного регулювання має зробити заяву та рішуче спростувати цю інформацію і навіть запросити представників МАГАТЕ. Для внутрішньої аудиторії повинна бути реакція від Центру з протидії дезінформації Ради національної безпеки і оборони щодо спростування фейкових наративів, аби заспокоїти населення та запобігти паніці. Серед обговорюваних механізмів були вказані престури для журналістів, роз'яснювальна робота з громадськістю, завчасне інформування про захист інших атомних електростанцій, достатню кількість палива, пункти вимірювання радіації та інформування населення про дії Бастана.

Ввідна 3.4.5: День 56: 2 березня, 16:00

Бастан встановлює зону контролю, де кораблі, що прямують у Сенту, зупиняються й обшуковуються військово-морськими силами Бастана, береговою охороною або обома відомствами. Мотивацією таких дій, як оголосив Бастан, є підозрювана терористична загроза невизначеним стратегічним

цільм. Кораблі піддаються вибіркового контролю. Затримки варіюються від п'яти годин до двох днів. Середній час очікування одного корабля становить 20 годин.



Реагування на Ввідну 3.4.5

Спочатку обговорювалися наслідки: економічна криза посилюється, втрати іміджу Сенти на міжнародній арені зростають, зростає соціальна напруженість та існує цілком реальна ймовірність ескалації ситуації з Бастаном. Далі обговорювалися основні завдання: відновити судноплавство, заспокоїти міжнародних партнерів і знизити соціальну напруженість. Кроки для досягнення цих завдань: поширення нарративів СТРАТКОМ через МЗС для міжнародної аудиторії (в тому числі партнерів і Бастана), які доводять партнерам, що така ситуація заснована на фейкових приводах і що Бастан порушує міжнародне право, а також поширення позитивного нарративу, що розповідає про події з точки зору Сенти. Ці наративи також повинні бути включені до повідомлень, які надсилаються Міністерством оборони та обласною державною адміністрацією.

6.4. Епізод 4: Гібридна війна

Напруженість у відносинах між Бастаном і Сентою досягла найвищого рівня за всю їх історію. Військова розвідка Сенти повідомила про безпрецедентне нарощування військових сил і засобів на базах бастанського флоту в морі Нуар. На острові Тотара почала відбуватися значна кількість провокаційних нещасних випадків. Повідомлення про втрату сигналів GPS і GSM на острові. Підключення до Інтернету на острові зникло.

У той самий час Сента продовжує стикатися зі збільшенням кількості кібератак на урядові та місцеві установи та постачальників критично важливих послуг. ЗМІ Бастана і Сенти повідомляють в агресивній манері про нездатність центральної та місцевої влади Сенти надавати населенню критично важливі послуги. Більш того, вищі командири Збройних сил Сенти в Києві та посадові особи Військово-морських сил в Одесі та на острові Тотара отримали електронні листи з непідтверджених профілів з прямим попередженням «не виконувати накази політичного керівництва Сенти, інакше вони та їхні сім'ї будуть в небезпеці».

Соціальні мережі сповнені повідомлень і активних дискусій про можливе відділення південної частини Сенти. Ті ж новини поширюються через офіційні вебсторінки регіональних рад. Все вищевказане призводить до тиску та напруження всередині державних установ, правоохоронних органів і збройних сил. За останні 24 години різко посилюються вуличні демонстрації проти уряду Сенти, а саме в центральних містах південних регіонів: Одесі, Миколаєві та Херсоні. В результаті уряд функціонує на межі можливого, а населення збентежене.

На тлі значних кібератак, психологічного тиску, поширення дезінформації і дедалі більших вуличних протестів у південних регіонах на острові Тотара раптово висадилася значна кількість о/с збройних сил без розпізнавальних знаків. Доступ до порту острова Тотара заблокований вантажними суднами без розпізнавальних знаків і прапора держави. Доступ по воді до острова Тотара відрізаний. Бурові установки для видобутку вуглеводнів на острові Тотара, розташовані у ВЕЗ Сента, були захоплені й тепер знаходяться під повним контролем озброєних людей без розпізнавальних знаків.

Ввідна 4.4.1: День 56: 2 березня, 05:00

Озброєні люди без розпізнавальних знаків захопили вісім газових вишок біля острова Тотара у ВЕЗ Сенти. Вони десантувалися на вишки за допомогою вертольотів і захопили їх. Військово-морські сили Бастана встановлюють зону контролю навколо бурових установок, а саме в районах Штурмівського і Голіцинського газових родовищ. Цивільні судна й літаки повідомляють про значний збій у роботі GPS-сигналів в районі моря Нуар.

Реагування на Ввідну 4.4.1

Обговорюються наслідки кризи: втрата критичної інфраструктури, поглиблення економічної кризи, закриття повітряного і морського сполучення, а також соціальна напруженість, що зростає. Основні завдання, які визначив Синдикат, включають заклик до всіх міжнародних партнерів збільшити свою присутність в цьому районі та об'єднати країни проти суб'єкта, відповідального за ситуацію: Бастана. Потім був обговорений аналіз цільової аудиторії: хто може бути партнером в деескалації кризи, хто може надати інформаційну підтримку, аби донести повідомлення до різних аудиторій, хто може надати словесну підтримку Сенті, хто не буде коментувати ситуацію і хто буде виступати проти Сенти. Тим часом повинна бути підготовка повідомлень для деескалації поточної кризи, як оголосити про

успішне завершення операції, з можливою одночасною заявою Президента разом з партнерами. Мають бути забезпечені суворі заходи безпеки операцій під час всіх дій і заходів з одночасним висвітленням того, що відбувається, в інформаційному просторі, в тому числі міжнародному і ворожому.

СБУ повинна провести антитерористичну операцію та очолити дії щодо цієї кризи. Додаткова підтримка повинна бути структурована таким чином:

1. Засідання Ради національної безпеки і оборони
2. МЗС: ініціатива щодо залучення міжнародних організацій.
3. Збори територіальної оборони - у всіх регіонах, аби об'єднати Сенту проти Бастана.
4. Превентивні заходи, аби Бастан не виставляв себе жертвою.
5. Міністерство закордонних справ має визначити країни, які будуть підтримувати, і ті, які не будуть створювати різні повідомлення для різних міжнародних аудиторій. Слід також створити коаліцію держав, які підтримають Сенту, висвітливши підтримку в інформаційному просторі спільними двосторонніми та багатосторонніми заявами.
6. Міністерство оборони має запустити інформаційні операції для підтримки населення острова Тотара, в тому числі для військових, які знаходяться там
7. Внутрішня аудиторія - всі військовослужбовці Сенти та їхні родичі повинні бути заспокоєні.
8. Розвіддані іноземних партнерів повинні допомогти у встановленні причетності Бастана.
9. Залучення громадськості за допомогою навчання діям в надзвичайних ситуаціях, громадської безпеки тощо, коротких відеороликів в соціальних мережах, що висвітлюють правду про ситуацію на острові Тотара. Місцеве населення має отримати інструкції з надання першої допомоги та виявлення небезпечних предметів.

Ввідна 4.4.2: День 58: 4 березня, 02:00

На острів Тотара десантується значна кількість добре озброєних людей без розпізнавальних знаків.

Повідомлення про захоплення місцевих установ і основної військово-морської бази Сенти на острові. Влада Бастана заперечує будь-яку причетність до цієї операції. Телевізійні ЗМІ Бастана звинувачують ультраправі сили Сенти в геноциді місцевого населення. В цей час на острові відсутній Інтернет і GSM-покриття.

Водночас на вебсайті парламенту Тотари повідомляється, що з метою захисту місцевого населення від геноциду з боку ультраправих сил Сенти влада острова приймає рішення оголосити про відокремлення від Сенти та звертається до Бастана за допомогою.



Реагування на Ввідну 4.4.2

Спочатку знову обговорювалися наслідки: тривале порушення територіальної цілісності Сенти, дестабілізація і соціальна напруженість, ймовірність відкритого військового конфлікту, загострення економічної кризи, повне блокування морського сполучення і загроза втрати міжнародної підтримки, і все це в результаті гібридних дій Бастана. Важливість комунікації тут не можна недооцінювати. Потім були обговорені основні завдання: відновлення територіальної цілісності, судове переслідування Бастана за порушення ним міжнародного права і відновлення іміджу Сенти на міжнародній арені. Основними зовнішніми аудиторіями є діаспора (Світовий конгрес українців) і ООН (офіційне повідомлення про право на застосування сили). Для внутрішньої аудиторії пріоритет віддається Збройним силам на острові Тотара і решті території, їх родичам, а також нейтральному, пробастанському і протестуючому населенню. Також пропонується залучити церкви та релігійні організації до інформування суспільства. Повідомлення, скеровані на аудиторії, повинні бути різного ступеня: у нас є право застосовувати силу, це не громадянська війна, це зовнішня агресія Бастана, і на острові Тотара немає геноциду.

6.5. Епізод 5: Посткризова стабілізація

Цей епізод присвячений посткризовому відновленню та процесу стабілізації. Посткризова стабілізація відбувається після закінчення кризового сценарію – з 7 березня 20XX року. Також потрібно обговорити питання управління в кризових ситуаціях.

Кожному синдикату буде запропоновано кілька питань для обговорення посткризової стабілізації.

1. Чи існує ефективна система стратегічних, в тому числі кризових, комунікацій? Як ви забезпечуєте ефективну і надійну стратегічну комунікацію із зовнішнім світом? Які основні проблеми/виклики у сфері стратегічних комунікацій?
2. Які шляхи поліпшення наявної системи? Чи вимагає це додаткових елементів, які зараз відсутні?
3. Як би ви виявляли, аналізували та протидіяли кампаніям з дезінформації для внутрішньої та зовнішньої аудиторії?
4. Які ви бачите шляхи залучення державного і приватного секторів в систему стратегічних комунікацій?

Синдикат не завершив Епізод 5.

6.6. Ключові висновки

Створити офіс СТРАТКОМ на рівні уряду. З точки зору СТРАТКОМ Україна дуже добре знає противника і знає, як Росія проводить гібридні операції. Однак у нього немає протоколів, інститутів і механізмів для своєчасного, скоординованого та ефективного реагування. Багато учасників визнали, що відсутні: 1) чітке керівництво для координації зусиль елементів СТРАТКОМ, які існують в різних організаціях, 2) міжвідомча комунікація і координація та 3) механізми комунікації та координації між приватним сектором і Урядом. Ця відсутність перешкоджає ефективному реагуванню на кризові ситуації на стратегічному рівні. Немає чітко визначеної функції на рівні уряду в жодного з міністерств / відомств для організації розрізнених груп з метою створення єдиної комунікаційної стратегії або для координації зусиль кожної групи на підтримку цієї загальної стратегії. Як результат, їм необхідно створювати спеціальну команду для кожної кризи, що є повільним і неефективним процесом. З точки зору наративів реагування СТРАТКОМ, швидкість і гнучкість в обміні повідомленнями, можливо, є найбільш важливою частиною досягнення їх основних завдань. **Рекомендація(ї):** Створити офіс СТРАТКОМ на рівні уряду з чітким і єдиним керівництвом, який функціонує як об'єднане відомство для створення стандартизованих наративів для внутрішньої, міжнародної та ворожої аудиторії. Синдикат рекомендував створити незалежну національну посаду з кризових комунікацій на рівні уряду безпосередньо при Прем'єр-міністрі. Рекомендуємо впровадити цю посаду і зробити її постійною, безперервною службою, а не спеціальною командою, яка створюється тільки для координації кожної окремої кризи, що виникає.

Удосконалити та укласти протоколи і процедури СТРАТКОМ для швидкого й узгодженого реагування на кризи. Національні плани, регламенти та процедури антикризового управління для реагування і зменшення наслідків і впливів гібридних дій, мабуть, є найбільш потрібним аспектом нинішньої структури СТРАТКОМ в Україні, який нині відсутній. Зараз в Україні немає базових протоколів або механізмів для швидкого реагування на гібридні загрози. На додаток до відсутності єдиного центру керівництва та координації, як згадувалося вище, зараз вони неефективні як у визначенні рівня і типу необхідних заходів, так і у створенні наративів для різних відповідних аудиторій, коли виникають гібридні кризи. Синдикат відзначив відсутність або неадекватність механізмів координації між установами, відсутність визначень рівнів класифікації криз, недостатню кількість державних каналів зв'язку з населенням і відсутність будь-якої заздалегідь визначеної системи оповіщення громадськості. Перебої в подачі електроенергії, перебої в роботі транспорту, атаки типу «відмова в обслуговуванні», потік дезінформації в соціальних мережах і російських державних ЗМІ, а також цілеспрямовані загрози окремим громадянам за допомогою цифрових технологій – все це було частиною гібридних дій росії проти України. Якщо криза коли-небудь переросте в гібридну війну, то росія, безумовно, використає всі свої можливості для порушення і

погіршення зв'язку, аби ще більше посіяти хаос і безладдя серед українського уряду і населення. СТРАТКОМ повинен бути готовий до цих збоїв і мати плани дій на випадок непередбачених обставин, аби передавати свої повідомлення в таких обставинах. **Рекомендація(ї):** Розробити протоколи та структуру й кодифікувати їх у державних регламентах/законах, аби не було необхідності створювати їх в умовах кризи. Включити класифікацію типів криз за ступенем серйозності та які державні та приватні організації необхідно залучати для кожного типу, а також певні рівні реагування, які включають в себе, зокрема такі питання: хто буде передавати повідомлення і по яких каналах. Стандартні процедури та попередньо затверджені протоколи можуть скоротити час реагування, що дозволить керівництву краще зрозуміти ситуацію. Впровадити протоколи оцінки ризиків, аби різні аудиторії могли зрозуміти серйозність кризи й те, як вона впливає на них. Впровадити протоколи зв'язку в кризових ситуаціях, аби мати можливість спілкуватися через стаціонарний телефон, радіо, поштовий зв'язок і навіть за допомогою листівок, аби охопити аудиторію в екстремальних обставинах. Ці плани дій у надзвичайних ситуаціях мають вирішальне значення для запобігання заворушенням і паніці серед населення у разі виникнення сценарію гібридної війни.

Розробити стандартний метод планування СТРАТКОМ, у тому числі стратегічні наративи, що стосуються внутрішніх, міжнародних і ворожих наративів. Українські елементи мають чітке розуміння обміну повідомленнями на тактичному рівні, але не мають загальних рамок для управління зусиллями з обміну повідомленнями під час кризи. Кожна організація має свої власні стандартні методи планування і таргетування СТРАТКОМ без чіткого поділу повідомлень на організаційному рівні, наприклад, для цільової аудиторії (внутрішньої/міжнародної/ворожої). Їм потрібно вирішити, якого результату вони хочуть, які наративи розробити для кожної цільової аудиторії, яких ефектів вони очікують і як їх своєчасно реалізувати. Навіть після того, як будуть розроблені чіткі протоколи під керівництвом директора з комунікацій на рівні уряду, все одно буде необхідно швидко розробляти й поширювати повідомлення, що відповідатимуть стратегічним темам. **Рекомендація(ї):** Створити модель, яка забезпечує загальний метод планування та розповсюдження стратегічних комунікацій (наприклад, бажаний результат, цільова аудиторія, очікувані ефекти та виконання). Зокрема, елементи СТРАТКОМ повинні структурувати свої зусилля в рамках деякої варіації моделі «Активність -> Аудиторія -> Повідомлення -> Сприйняття -> Бажаний Результат». Розробити попередньо затверджені теми повідомлень на основі певних рівнів кризи, які можуть бути швидко поширені при необхідності. Що вони говорять своїм різним внутрішнім аудиторіям? Як вони спілкуються зі своїми західними союзниками та партнерами? Які заходи слід вжити, аби зменшити наслідки наративу, що лунає від противника? Це питання, які слід задавати перед кожною кампанією надання публічних повідомлень, а для налагодження співпраці між різними залученими організаціями у них повинен бути загальний метод підходу.

Плануйте заздалегідь і завжди будьте на стратегічному рівні. Національні плани, регламенти та процедури антикризового управління для реагування і зменшення наслідків і впливів гібридних дій, мабуть, є найбільш потрібним аспектом нинішньої структури СТРАТКОМ в Україні, який нині відсутній. Зараз в Україні немає базових протоколів або механізмів для швидкого реагування на гібридні загрози. На додаток до відсутності єдиного центру керівництва та координації, як згадувалося вище, зараз вони неефективні як у визначенні рівня і типу необхідних заходів, так і у створенні наративів для різних відповідних аудиторій, коли виникають гібридні кризи. Синдикат відзначив відсутність або неадекватність механізмів координації між установами, відсутність визначень рівнів класифікації криз, недостатню кількість державних каналів зв'язку з населенням і відсутність будь-якої заздалегідь визначеної системи оповіщення громадськості. Перебої в подачі електроенергії, перебої в роботі транспорту, атаки типу «відмова в обслуговуванні», потік

дезінформації в соціальних мережах і російських державних ЗМІ, а також цілеспрямовані загрози окремим громадянам за допомогою цифрових технологій - все це було частиною гібридних дій росії проти України. Якщо криза коли-небудь переросте в гібридну війну, то росія, безумовно, використає всі свої можливості для порушення і погіршення зв'язку, аби ще більше посіяти хаос і безладдя серед українського уряду і населення. СТРАТКОМ повинен бути готовий до цих збоїв і мати плани дій на випадок непередбачених обставин, аби передавати свої повідомлення в таких обставинах.

Рекомендація(ї): Розробити протоколи та структуру й кодифікувати їх у державних регламентах/законах, аби не було необхідності створювати їх в умовах кризи. Включити класифікацію типів криз за ступенем серйозності та які державні та приватні організації необхідно залучати для кожного типу, а також певні рівні реагування, які включають в себе, зокрема такі питання: хто буде передавати повідомлення і по яких каналах. Стандартні процедури та попередньо затверджені протоколи можуть скоротити час реагування, що дозволить керівництву краще зрозуміти ситуацію. Впровадити протоколи оцінки ризиків, аби різні аудиторії могли зрозуміти серйозність кризи й те, як вона впливає на них. Впровадити протоколи зв'язку в кризових ситуаціях, аби мати можливість спілкуватися через стаціонарний телефон, радіо, поштовий зв'язок і навіть за допомогою листівок, аби охопити аудиторію в екстремальних обставинах. Ці плани дій у надзвичайних ситуаціях мають вирішальне значення для запобігання заворушенням і паніці серед населення у разі виникнення сценарію гібридної війни.

7. Синдикат 5: Міжнародне реагування/Міжнародне право



Синдикат «Міжнародне право» обговорює «ключові висновки», сформульовані під час виконання КШН CORE 20 в Одесі, Україна.

7.1. Епізод 1: Доконфліктна фаза: Гібридний вплив

Посилюється політичне та економічне залякування з боку влади Бастану. На підставі угоди про транзит газу, яка була підписана між Бастаном і Сентою минулого року, уряд Бастану звинуватив Сенту в порушенні положень угоди. Сента заперечує будь-які порушення. Однак ЗМІ Бастану і деякі ЗМІ Сенти, контрольовані Бастаном, продовжують поширювати повідомлення про порушення Сенти, підкреслюючи важливість відповідної угоди для енергетичної безпеки Європи, оскільки транзит газу в європейські країни частково забезпечується через територію Сенти.

Ситуацію ускладнює той факт, що між Бастаном і Велою не укладено новий контракт на постачання газу. Враховуючи суперечки щодо договірних положень, Бастан тимчасово істотно скорочує постачання газу в Велу. Вела максимально відбирає газ з транзитного трубопроводу, обмежуючи постачання газу споживачам Сенти в Одеській області, недалеко від кордону з Румунією.

Тим часом Бастан ввів обмеження на імпорт сільськогосподарських, промислових товарів та металевих виробів, палива, хімікатів і нафтопродуктів із Сенти. Крім того, Бастан припиняє постачати нафтопродукти в Сенту автомобільним, залізничним транспортом і трубопроводами.

В Інтернеті були виявлені три вебсайти з ідентичним візуальним оформленням і функціями офіційних вебсайтів Оператора ГТС Сенти, Оператора PSG і компанії «Нафтогаз». Крім того, на електронні адреси регіональних урядових установ Сенти були надіслані листи з фішинговими функціями та прикріплені текстові документи Microsoft Word.

У ЗМІ з'явилися повідомлення про потужну кібератаку на внутрішню мережу Liebherr в Німеччині. В результаті портові крани в морському порту Поті в Зестані перестали працювати.

З середини грудня берегова охорона Сенти регулярно повідомляє про присутність Військово-морських сил Бастану у ВЕЗ Сенти. Повідомляється, що Бастан проводив військові навчання в морі

Нуар у безпосередній близькості від фарватерного проходу торгових і пасажирських суден з/в порти Одеської області.

Ввідна 1.5.1: День 1: 6 січня, 11:00

Через рік після підписання угоди про транзит газу влада Бастана звинувачує Сенту в порушенні угоди, попереджаючи про розірвання контракту і припинення постачання газу через територію Сенти.

Реагування на Ввідну 1.5.1

Було піднято питання про те, чи підписання угоди, яка ще не ратифікована, робить її юридично обов'язковою, і було вирішено вважати, що вона має юридичну силу для цього сценарію. Сента повинна розуміти, щодо порушення яких частин угод Бастан її звинувачує, що вимагає від газових компаній і уряду Сенти можливості швидкого й ефективного спілкування. Ситуація складна, тому що в цьому беруть участь дві сторони: комерційні газові компанії та уряд Сенти, зокрема міністр закордонних справ (МЗС) і міністр енергетики (Міненерго). Газові компанії повинні відреагувати на ці звинувачення, але, оскільки вони є комерційними структурами, то уряд також повинен забезпечити надсилання чіткого уніфікованого повідомлення населенню та міжнародній спільноті. Інша проблема полягає в тому, що газ просто транспортується транзитом через Сенту в інші держави (зокрема, в країни ЄС). Постачальники газу з цих інших країн також матимуть можливість показати, чи дійсно вони бачать проблеми, що робить доведення інформації до міжнародної спільноти ще більш важливим питанням. Сента не повинна дозволяти Бастану керувати інформаційною картиною, особливо якщо ця інформація неправдива. Важливо, аби будь-яка інформація, що розповсюджується Сентою в комерційній або офіційній сфері, показувала, що бізнес ведеться відповідно до вимог і зобов'язання фактично виконуються, і це повинно бути просто інформаційним, а не реакційним; Сента повинна показати своїм сусідам, що вона компетентна і надійна.

Рекомендація: Здатність реагувати та метод реагування повинні бути частиною політики. Ця політика повинна бути розроблена до виникнення інцидентів і бути чітко зрозумілою постачальникам, пов'язаним з критичною інфраструктурою, а також уряду Сенти. Ці сторони, що залучені до сфери критичної інфраструктури (в цьому випадку газові компанії), повинні бути залучені в розробку цього плану, аби забезпечити його ефективність при використанні в разі необхідності. З метою швидкого реагування в уряді Сенти повинен бути створений Державно-приватний координаційний орган (очолюваний Міністерством закордонних справ або Міністерством інформаційної політики) як докризовий центр, аби скоротити час реагування з тижня до декількох годин.

Рекомендація: Важливо забезпечити випуск та розміщення Сентою в Інтернеті пресрелізів і заяв не тільки українською, але й англійською та іншими іноземними мовами. Зокрема, англійська версія була б корисною для забезпечення того, аби міжнародна спільнота могла відразу зрозуміти ситуацію та бути проінформованою про неї. Коли інформація публікується тільки українською мовою, це перешкоджає можливості швидкого міжнародного реагування, створюючи завади у наданні допомоги, яку б в іншому випадку могла отримати Сента, аби не було затримок з перекладом. Члени Синдикату кажуть, що «Англійську версію новин можна відправити в Google, і звідти вона швидко пошириться всім іншим».

Рекомендація: Національний план дій з газопостачання Сенти необхідно оновлювати щороку. Дати можливість країнам ЄС здійснювати закупівлі газу безпосередньо на кордоні Сента-Бастан, аби показати Сенту як надійного постачальника газу і мінімізувати транзитні ризики.

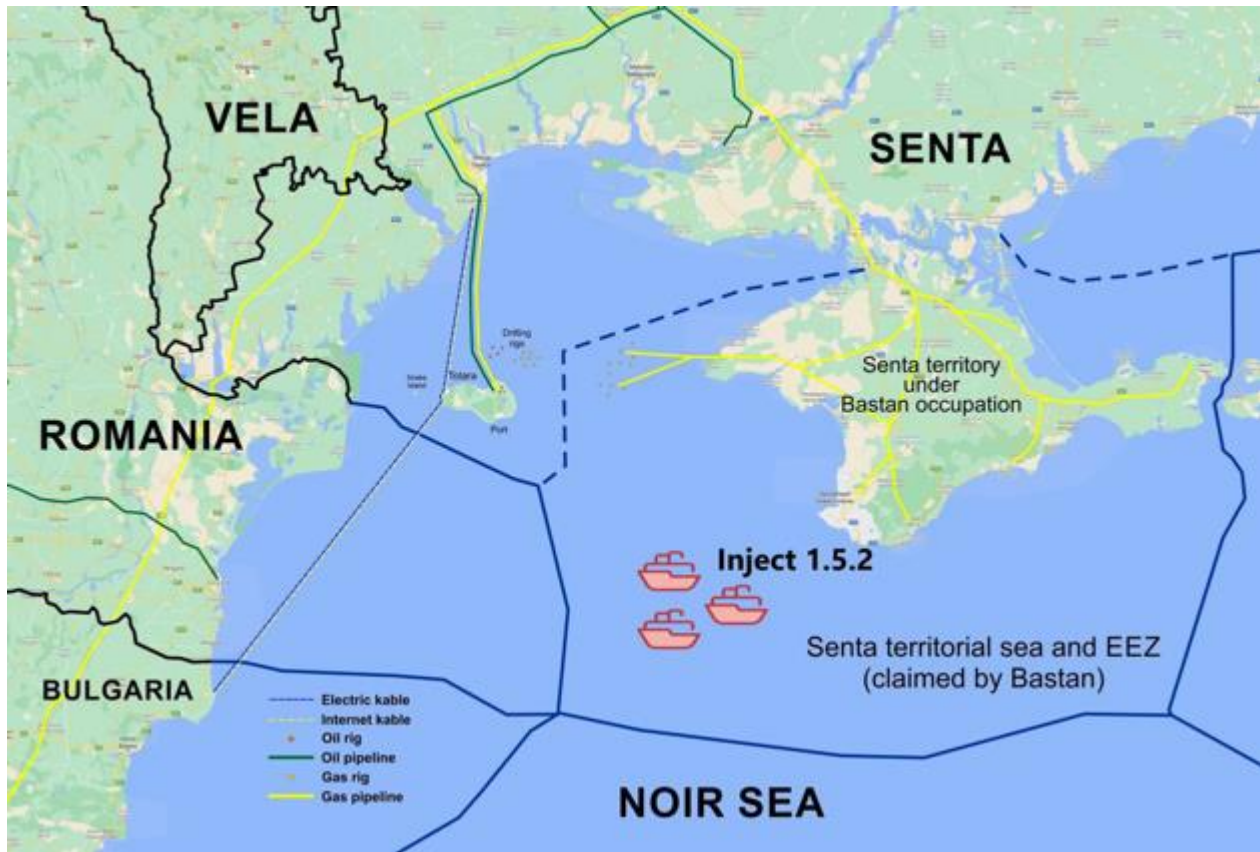
Рекомендація: Надання інформаційної відповіді на звинувачення має бути негайним, а не відкладатися в очікуванні отримання всіх фактів, перш ніж реагувати. Така затримка в часі завдає шкоди Сенті. Необхідно швидко реагувати, аби проінформувати міжнародну спільноту про ситуацію в тому вигляді, в якому вона зараз відома Сенті, а після цього може бути надана додаткова розширена інформація. Очікування для з'ясування всіх фактів і мовчання надають повідомленням Бастана більшої ваги, навіть якщо вони не відповідають дійсності. Навіть якщо всі факти невідомі та необхідне подальше розслідування, Сента може опублікувати заяву, засновану на принципах (наприклад, борги будуть виплачені, умови контрактів будуть дотримані, буде повне і відкрите розслідування тощо).

Рекомендація: Слід створити групи швидкого реагування на державному кордоні для забезпечення швидкого реагування при виникненні загрози безпеці або миру, аби звести загрози до мінімуму. Зараз багато угод про прикордонне міждержавне співробітництво передбачають проведення зустрічей, які організуються всього кілька разів на рік. Є необхідність у постійному методі швидкого зв'язку між прикордонними державами для реагування на кризові ситуації.

Рекомендація: Забезпечити діяльність РНБО відповідно до Указу Президента № 115 від 28 лютого 2015 року як головного органу управління для виявлення кризової ситуації та створення Кризового центру під головуванням Секретаря РНБО.

Ввідна 1.5.2: День 5: 10 січня, 10:00

Військово-морські сили Бастана присутні у ВЕЗ Сенти, а кораблі не відповідають на інформаційні запити берегової охорони Сенти. Кораблі ВМС Бастана також переслідують комерційні судна, що проходять транзитом в Одеський морський порт, під приводом «проведення операції із забезпечення безпеки».



Реагування на Ввідну 1.5.2

Сента повинна реагувати кожного разу, коли порушуються ці закони, навіть якщо це відбувається постійно. Необхідно звернутися до країн-партнерів за допомогою в патрулюванні та забезпеченні правильності думок і бачень країн-партнерів, Сента не повинна дозволяти Бастану контролювати інформацію, яку бачать країни-партнери. Залучення країн-партнерів гарантує, що вони також зможуть надати інформацію і показати, що відбувається в морі Нуар. Зупинка Бастаном кораблів у ВЕЗ Сенти заборонена. Спільне патрулювання ВЕЗ має життєво важливе значення. Коли відбувається порушення державних кордонів, повинна бути залучена РНБО, яка надасть подальші рекомендації. РНБО не дає вказівок президентській гілці влади й тому виникає питання, чи існує чіткий план того, що слід робити, коли відбувається порушення ВЕЗ. Є Кодекс цивільного захисту, але він застарів (створений за часів імперії Понуксін), проте він передбачає заходи реагування в надзвичайних ситуаціях.

Рекомендація: Потрібне оновлення Кодексу цивільного захисту, що може забезпечити внутрішній план реагування на загрози. Його необхідно доповнити кризовими сценаріями, аби забезпечити Національний план реагування. Зокрема, розробка конкретних заходів реагування на кризові ситуації у разі порушення ВЕЗ з моря.

Рекомендація: Важливо, аби переслідування комерційного судноплавства розглядалося як питання державної безпеки, а не як комерційний правовий спір. Міністерство закордонних справ має

забезпечити, аби комерційні контракти, що стосуються судноплавства, чітко й прямо визначали право уряду Сенти втручатися.

Рекомендація: Забезпечити наявність перевіреного та ефективного механізму прямого і негайного інформування міжнародних партнерів (НАТО і партнерів по прикордонних морських районах) про ці типи суперечок. Старі угоди про дружбу/партнерство радянської епохи з прикордонними країнами можна було б оновити та використовувати для створення механізмів консультацій і надання допомоги. Після цього угоди можна було б щорічно переглядати.

Рекомендація: Сенті слід стандартизувати свою здатність без зволікання звертатися до НАТО відповідно до пункту 15 своєї угоди про партнерство з НАТО, коли виникають проблеми стосовно територіальної цілісності. А з екстремими зустрічами з НАТО взагалі не повинно бути проблем. Сенті слід послідовно використовувати пункт 15.

Рекомендація: Сенті слід укласти угоди про морське патрулювання і налагодити співпрацю зі своїми морськими сусідами, аби забезпечити багатостороннє реагування в подібних ситуаціях. Патрулювання прибережних районів коаліцією має стати звичайною справою до того, як виникне криза. Сенті необхідно домагатися укладання таких угод якомога швидше.

Рекомендація: Сенті слід організувати можливості обміну/стипендіальні програми між Сентою і країнами НАТО/ЄС для обміну ідеями та вивчення проблем, пов'язаних з гібридною війною, до виникнення конфліктів.

7.2. Епізод 2: Гібридні операції низької інтенсивності

На початку лютого погодні умови в південних районах Сенти погіршилися. Швидкість вітру досягає 50 м/с, що завдає значної шкоди, зокрема, в Одеській області.

Введені Бастаном обмеження на імпорт сільськогосподарських, промислових товарів та металевих виробів, палива, хімікатів і нафтопродуктів із Сенти сприяють занепаду економіки Сенти, яка вже знаходиться в стані рецесії. Пробастанські активісти використовують економічний спад як шанс посилити протести проти уряду Сенти. Соціальна напруженість досягла свого піка, коли в Інтернеті поширилася новина про рішення Одеської міської ради про вихід Одеської області зі складу Сенти.

Діяльність пробастанських активістів та інциденти у сфері кібербезпеки постійно порушують роботу Одеського морського порту. Крім того, цивільні судна і кораблі берегової охорони Сенти повідомляли про технічні неполадки у роботі своїх навігаційних систем.

Крім того, судна Бастана діють агресивно проти риболовецьких суден Сенти. Кораблі берегової охорони Бастана залякують і погрожують вантажним суднам Сенти, а також суднам іноземних держав. Нещодавно Військово-морські сили Бастана надали підтримку незаконній діяльності з розвідки газу та встановлення бурових установок на території ВЕЗ Сенти. Навколо бурових установок був встановлений цілодобовий охоронний патруль Військово-морських сил Бастана.

Відна 2.5.1: День 43: 17 лютого, 10:00

Через суворі погодні умови, а саме сильний вітер зі швидкістю 50 м/с, танкер, що належить Сенті, раптово втратив управління і зіткнувся з вантажним судном Бастана у ВЕЗ Сенти, що призвело до витоку нафти та значної пожежі. Повідомляється про декількох постраждалих. Бастан звинувачує владу Сенти в диверсії.

Реагування на Ввідну 2.5.1

Існує протокол щодо забруднення моря Нуар. Сенті слід звернутися до країн НАТО і країн в морі Нуар за допомогою у ліквідації наслідків розливу. Високорівневий формат центру швидкого реагування не працює. Потрібна робоча група, яка займається тільки надзвичайними ситуаціями та складається з декількох міністерств, аби могла функціонувати. Ймовірно, що Міністерство захисту довкілля та природних ресурсів Сенти (Міндовкілля) і Міністерство інфраструктури Сенти візьмуть на себе провідну роль. Однак Міндовкілля втратить свою роль головного органу в ситуації, коли буде встановлено, що це криза.

Рекомендація: Створити механізм для інформаційних запитів від відомств Сенти до Міністра закордонних справ про їхні потреби з боку міжнародних організацій. Це забезпечить кращу координацію. Такий механізм забезпечить швидке розуміння з боку МЗС, що саме найбільше допоможе відомствам Сенти, аби МЗС міг швидко отримати допомогу від міжнародної спільноти та переконатися, що це той тип допомоги, який найбільш необхідний. Донесення чіткої інформації до міжнародних ЗМІ про ворожу поведінку є дуже важливим. Не дозволяйте наративу Бастана залишитися без відповіді.

Рекомендація: МЗС слід забезпечити наявність ефективних і швидких комунікаційних можливостей Сенти з міжнародними аналітичними центрами, аби поліпшити розподіл своїх комунікацій і повідомлень. Крім того, Сенті слід провести ретельні дослідження за участю декількох аналітичних центрів для розробки ймовірних сценаріїв і планів реагування на ці типи Епізодів (стосується Епізоду 2/3/4/5).

Рекомендація: Знову ж таки, Сенті слід стандартизувати свою здатність без зволікання звертатися до НАТО відповідно до пункту 15 своєї угоди про партнерство з НАТО, коли виникають проблеми територіальної цілісності. Екстрені зустрічі з НАТО не повинні викликати жодних проблем, але радше Сента повинна використовувати пункт 15. Запити на спільне патрулювання з НАТО повинні бути стандартизовані.

Рекомендація: Переглянути питання про те, яке відомство Сенти виконуватиме керівну роль у зв'язку з подією, яка не є «чистою надзвичайною ситуацією», а являє собою невідкладну проблему, що вимагає швидких і скоординованих дій. Можливо, Міндовкілля не найкращий вибір.

Рекомендація: Сенті слід посилити спроможності розвідувальних служб і посилити взаємодію з ЄС і НАТО в питаннях розвідки. Сенті слід прагнути значно підвищити ефективність своєї розвідувальної роботи.

Відна 2.5.2: День 46: 20 лютого, 17:00

Кораблі берегової охорони Сенти інформують про дії Бастана в морі Нуар. Останнім часом Бастан встановив газові самопідйомні бурові установки, проводячи розвідку і видобуток газу на території континентального шельфу Сенти. Кораблі ВМС Бастана патрулюють навколо газових вишок.

Реагування на Ввідну 2.5.2

Необхідно скликати РНБО та апелювати до міжнародних законів стосовно того, що Бастан буде бурові установки у ВЕЗ Сенти. Хоча це не визнано міжнародною спільнотою законним, проте Бастан стверджує, що у нього є таке право і воно базується на тому, що Сента незаконно захопила ці землі. Таким чином, Бастан не має права стверджувати, що вони захищають свої власні економічні інтереси. Конвенція з морського права накладає двосторонні зобов'язання. Сенті слід проконсультуватися зі своїми партнерами та використовувати їх бачення дій в приватному і державному секторах, аби вказати на те, що робить Бастан, і на проблеми, які він створює, перешкоджаючи комерційному судноплавству у ВЕЗ Сенти. Реальна мета полягає в тому, аби гарантувати, що Сента отримає допомогу в разі проблем, викликаних діями ворожої держави. Збір інформації має вирішальне значення, виконавча влада може забезпечити передачу всієї інформації РНБО. Існує особливий шлях подачі апеляції до Міжнародного суду і для цього питання. Розлив нафти становить загрозу для всього регіону, тому з цього питання Сента повинна оголосити про міжнародну зустріч, аби проінформувати представників країн, які можуть допомогти в ухваленні рішення про очищення, включаючи навіть Бастан. Що стосується Бастана, який встановлює самопідйомні бурові установки у ВЕЗ Сенти, то необхідно встановити правову основу для правил, які не дозволяють іншим країнам встановлювати самопідйомні бурові установки. Нам потрібно мати такі юридичні підстави, не дозволяючи Бастану продовжувати його дії, для того, аби Сента показала, що це незаконно і що у Бастана немає дозволу на такі дії у ВЕЗ Сенти.

Рекомендація: Має бути залучена міжнародна спільнота. Вона має знати про те, що відбувається, і правду про кричущі порушення Бастаном ВЕЗ Сенти. Пропонується долучити Організацію з безпеки та співробітництва в Європі (ОБСЄ).

Рекомендація: Постійно звертатися до міжнародних судів зі скаргами на порушення. Це дозволить тримати цей факт у центрі уваги міжнародної спільноти. Це також допомагає встановити бажану тенденцію щодо порушення закону стосовно того, що те, що робить Бастан, є незаконним. Переконайтеся, що процедури Сенти щодо швидкого подання заяв до міжнародних судів зрозумілі та відомі уряду Сенти.

Рекомендація: Міжнародній спільноті слід озвучити екологічні та торговельні наслідки від агресії. Слід забезпечити розуміння того, що Бастан не тільки веде військові дії проти Сенти, але й те, що дії Бастана також впливають на навколишнє середовище і торгівлю, економічні наслідки зачіпають не тільки Сенту. Має бути оприлюднена інформація про серйозні екологічні наслідки, аби забезпечити міжнародне співчуття.

Рекомендація: Сенті, європейським партнерам і союзникам по НАТО слід розглянути питання про те, як санкції та загроза санкцій можуть бути ефективно використані в подібних ситуаціях.

Рекомендація: Сенті слід провести детальне вивчення документів Європейського Союзу про принципи цивільного захисту, аби зрозуміти, чого вона може реально очікувати від ЄС в подібних ситуаціях.

Ввідна 2.5.3: День 48: 22 лютого, 07:00

Військово-Морські сили Бастана і берегова охорона залякують цивільні вантажні судна Сенти та Зестану, що прямують в порти Сенти в морі Нуар, перебуваючи у ВЕЗ Сенти, і вимагають, аби вони змінили курс назад до зовнішнього кордону ВЕЗ Сенти. Згідно з даними ЗМІ Бастана, цивільний вантажний корабель Сенти намагався навмисно врізатися в корабель ВМС Бастана. Ця інформація

була повторена Міністерством оборони Бастана, яке звинуватило кораблі Сенти в провокаційних і небезпечних діях. Згідно з повідомленнями ЗМІ Бастана, за таких обставин влада Бастана вирішила збільшити свою військово-морську присутність, аби захистити свої кораблі та інтереси від провокаційних дій Сенти.



Реагування на Ввідну 2.5.3

Пропонується використовувати засоби масової інформації, аби допомогти Сенті у цьому випадку. Бастан слід звинуватити в піратстві за порушення комерційного судноплавства. Міністерство оборони має підготувати пресреліз, а всі експерти повинні спробувати з'ясувати, що сталося, шляхом перевірки фактів. ЗМІ Бастана не слід довіряти. Прикордонна служба Сенти повинна повідомити, що сталося. Ставиться під сумнів, чи знаходиться ВЕЗ під відповідальністю і фіскальним контролем прикордонної служби. Військово-морські сили Сенти повинні мати можливість встановлювати визначені судноплавні шляхи, а зараз вони цього не зробили. Потрібно звернутися за допомогою до Туреччини, а також до міжнародної морської організації. Має бути залучене Міністерство інфраструктури, враховуючи, що мова йде про комерційні кораблі, разом з координацією з Міністерством закордонних справ і Міністерством оборони.

Рекомендація: Розробка чіткіше прописаних наказів, що визначають інші внутрішні методи уряду Сенти для швидкого збору, аналізу та передачі інформації міжнародній спільноті. Швидкий і повний внутрішній обмін інформацією життєво важливий, а процедури повинні бути встановлені заздалегідь, аби реагування відбувалося протягом декількох годин, якщо не менше.

Рекомендація: Обговорення й розробка плану спільних дій з країнами-партнерами та сусідніми державами стосовно дій, які необхідно вжити в таких кризових ситуаціях, з уже визначеними заходами та способами стримування.

Рекомендація: Уточнити міжнародне та внутрішнє законодавство про піратство. Розглянути можливість внесення проактивних змін у внутрішнє законодавство Сенти, аби гарантувати, що такого роду втручання в судноплавство вважається піратством. Може бути неможливим, якщо ворожі судна знаходяться під прапором Бастана.

Рекомендація: Поліпшити технічні можливості для обміну розвідувальною інформацією з регіональними морськими партнерами в рамках Партнерства розширених можливостей.

Рекомендація: Запросити військові кораблі НАТО взяти участь у навчаннях у морі Нуар, аби там були присутні інші міжнародні партнери, які могли б допомогти в стримуванні агресивної тактики Бастана. Потенційно також запросити міжнародних партнерів для допомоги в забезпеченні безпеки судноплавних шляхів для комерційних суден, що заходять в Одеський морський порт. Можливо, можна було б створити систему «Раптових навчань» з НАТО.

7.3. Епізод 3: Фаза конфлікту: Гібридні операції високої інтенсивності

Критична інфраструктура Сенти піддається широкому спектру ударів кінетичною і некінетичною зброєю. Перебої в роботі газопроводу з транспортування природного газу в Південному газотранспортному коридорі позначаються на постачаннях газу в Південний регіон Сенти та сусідні іноземні держави. Більш того, існує загроза зриву опалювального сезону не лише в південній частині Сенти, але й у Харківській і Луганській областях, які, зокрема, сильно залежать від постачання газу з Бастана.

На півдні Сенти на третину збільшилася кількість надзвичайних ситуацій, пожеж і нещасних випадків, викликаних підпалами й терористичними актами з використанням вибухових речовин, що, своєю чергою, призвело до значного збільшення числа постраждалих. Є підозра про масштабний інцидент на ПАТ «Одеський припортовий завод», де повідомляється про значний викид небезпечних хімічних речовин.

Поширюється інформація про збій в роботі Південно-Сентської АЕС. ЗМІ Бастана звинувачують владу Сенти у викидах радіації. Майже одночасно поширюється інформація про атаку на гідроакумуляуючу електростанцію.

Масовані кібератаки порушують роботу Одеського морського порту, в тому числі транспортування й обробку вантажів. Нападу зазнали банківські системи відділень Ощадбанку і ПриватБанку в Одеській області.

Через місяць після першої кібератаки на внутрішню мережу Liebherr в Німеччині сталася серія незначних кібератак на портові крани Liebherr по всій Європі.

У морській сфері кораблі ВМС Бастана збільшують свою присутність у ВЕЗ Сенти, використовуючи Військово-морські навчання, припиняючи міжнародні морські перевезення пасажирів і вантажів.

Ввідна 3.5.1: День 53: 27 лютого, 11:00

За останні п'ять днів, два вибухи потопили два вантажних судна, які належать Сенти та Зестану, що слідували в морський порт «Південний». Дві плавучі контактні міни часів Другої світової війни виявлені літаками-розвідниками та знищені Військово-морськими силами Сенти. Уряд Зестана публікує початкові технічні докази, що компрометують припущення про старі контактні міни: всі пошкодження розташовані глибше під корпусом, поруч з кормою, а всі вибухи відбулися в машинному відділенні. Деякі міжнародні судноплавні компанії оголошують ВЕЗ Сенти небезпечною для судноплавства.

Реагування на Ввідну 3.5.1

На відміну від попередніх ввідних, тепер Міністерству закордонних справ не потрібно враховувати інші міністерства. Тепер ми можемо легко підтвердити міжнародній спільноті, що сталися два вибухи, вони порушують ланцюжок постачання, і про це має бути відомо міжнародній спільноті. Досить очевидно, що необхідно донести повідомлення до міжнародної спільноти, аби отримати реакцію. Це повинні бути не тільки прес-релізи, всі наші посольства повинні бути негайно поінформовані, необхідно використовувати всі дипломатичні канали, аби всі негайно зрозуміли важливість і терміновість цього питання і те, що воно вийшло з-під контролю. Механізм ООН слід використовувати як частину Конвенції ООН з морського права щодо районів, які були заміновані.

Рекомендація: Забезпечити чіткість процесів зібрання Сентою послів вкрай важливих союзників у Києві для брифінгів у надзвичайній ситуації. Розглянути те, як організувати процес зустрічі послів союзників з посадовими особами Сенти для публічного заклику до розслідування або дій.

Ввідна 3.5.2: День 54: 28 лютого, 08:00

Великі вибухи на об'єктах з виробництва та зберігання аміаку ПАТ «Одеський припортовий завод». В результаті вибуху значний викид аміаку та інших небезпечних хімічних речовин в атмосферу. Повідомляється про десятки постраждалих на заводі. Отруйна хмара аміаку рухається в бік Одеси та сусідніх міст. Бастанські медіа та деякі ЗМІ Сенти повідомляють, що інцидент був інсценований як провокація службою безпеки Сенти.

Реагування на Ввідну 3.5.2

Міжнародні організації будуть негайно проінформовані про ситуацію, що склалася. Для розробки спільних заходів реагування на небезпечні викиди хімічних речовин слід використати спільну робочу групу з реагування на надзвичайні ситуації. Потрібно залучити НАТО. У нас є двостороння угода з нашими державами-партнерами щодо надзвичайних ситуацій, яку необхідно використовувати. Військові з країн-партнерів, які мають фахівців з питань небезпечних розливів, можуть надати допомогу – розглянути спроможності Європейського Союзу.

Рекомендація: Необхідно змінити та створити більш ефективну спільну робочу групу з партнерами ЄС з реагування на надзвичайні ситуації.

Ввідна 3.5.3: День 54: 28 лютого, 09:00

Військово-морські сили Бастана оголошують район стрільб і навчань небезпечним і блокують морський шлях в Одеський морський порт. Інтенсивні військові навчання, в тому числі з використанням різних систем озброєння, тривають вже два тижні та проводяться в безпосередній близькості до торгових суден, які проходять через цей район, що порушує судноплавство.

Реагування на Ввідну 3.5.3

МЗС має активізувати свою співпрацю з НАТО. Поточний процес працює, але це вимагає часу. Нам потрібно прискорити це, аби державні органи могли самостійно передавати інформацію в НАТО. На додаток до встановлених процедур необхідно використовувати кризовий центр як центр швидкого реагування. Термінові документи можуть бути відправлені безпосередньо в Офіс Президента. Як тільки оголошується надзвичайний стан, реагування відбувається швидше. Економічні наслідки постійних військових навчань бастанських ВМС, через які порушується судноплавство, повинні бути очевидні для міжнародної спільноти, а прохання про допомогу можуть ґрунтуватися на базі економічних наслідків.

Рекомендація: НАТО потребує дуже конкретного списку запитуваної допомоги, аби мати можливість швидко реагувати та надавати допомогу. Просто попросити про допомогу недостатньо, для НАТО потрібна чітка конкретика того, що необхідно. Слід розробити шаблон для інформування НАТО про допомогу для різних сценаріїв, аби забезпечити можливість швидкого реагування. Використовуйте модель квітня 2021 року, коли Україна звернулася з ефективним закликом до НАТО, коли російські війська зосередилися на сході.

Рекомендація: Використовувати колективний заклик всіх країн моря Нуар до ООН з вимогою, аби Бастан прибрав координати своїх навчань з морських шляхів, адже це викликає економічні потрясіння. Мета полягає в тому, аби привернути увагу до цієї проблеми на міжнародному рівні, навіть якщо нічого не зміниться.

Ввідна 3.5.4: День 55: 1 березня, 00:00

Підозрюється, що на Дністровську гідроакумуляючу електростанцію була здійснена кібератака. Після оновлення декількох програмованих логічних контролерів (ПЛК) зв'язок між виробничими процесами нестабільний. Оператору надаються нереалістичні дані про значення виробленої електроенергії. Крім того, раптово підіймаються всі ворота на максимальну висоту, викликаючи неконтрольований і незапланований витік води. Цей раптовий витік пошкоджує турбіни на гідроелектростанції, а також викликає швидку й масштабну повінь вниз по річці.

Ввідна 3.5.5: День 55: 1 березня, 11:00

Південно-Сентська атомна електростанція раптово вимушено переходить до аварійної зупинки. ЗМІ Бастана звинувачують постачальника ядерного палива з США, а «корумпована влада» Сенти повідомляє, що на атомній електростанції стався значний інцидент зі значним викидом радіації.



Ввідна 3.5.6: День 55: 1 березня, 12:00

Бастан встановлює зону контролю, де кораблі, що прямують у Сенту, зупиняються й обшуковуються військово-морськими силами Бастана, береговою охороною або обома відомствами. Мотивацією таких дій, як оголосив Бастан, є підозрювана терористична загроза невизначеним стратегічним цілям. Кораблі піддаються вибірковому контролю. Затримки варіюються від п'яти годин до двох днів. Середній час очікування одного корабля становить 20 годин.

Реагування на Ввідні 3.5.4/5/6

Гідроелектростанція залучить Міністерство енергетики та Державну службу з надзвичайних ситуацій Сенти. Річка постачає воду Сенті, а також Велі. Існує безліч угод про співпрацю у прибережній зоні моря Нуар, але необхідно зробити активні та практичні кроки для інформування про них та їх активації. Посилення інфотиску повинне відбутися якомога швидше, аби забезпечити участь консульств, що важко здійснити.

Рекомендація: Застарілі двосторонні угоди між Сентою і Румунією існують для захисту і повинні бути оновлені. Це буде ефективним способом отримання допомоги, але вони повинні включати дії щодо забезпечення залучення партнерів, способів надання допомоги та з якою метою.

Рекомендація: Слід негайно звернутися до Міжнародного агентства з атомної енергії, якщо є який-небудь натяк на втручання в ядерну інфраструктуру. Це призведе до значного та швидкого міжнародного реагування та залучення експертів в Сенту. Робіть таке звернення без вагань.

Рекомендація: Сенті слід прагнути приєднатися до Естонського Центру передового досвіду спільного кіберзахисту НАТО, аби краще розв'язувати питання кібербезпеки/гібридної війни.

7.4. Епізод 4: Гібридна війна

Напруженість у відносинах між Бастаном і Сентою досягла найвищого рівня за всю їх історію. Військова розвідка Сенти повідомила про безпрецедентне нарощування військових сил і засобів на базах Бастанського флоту в морі Нуар. На острові Тотара почала відбуватися значна кількість провокаційних нещасних випадків. Повідомлення про втрату сигналів GPS і GSM на острові. Підключення до Інтернету на острові зникло.

У той самий час Сента продовжує стикатися зі збільшенням кількості кібератак на урядові та місцеві установи та постачальників критично важливих послуг. ЗМІ Бастана і Сенти повідомляють в агресивній манері про нездатність центральної та місцевої влади Сенти надавати населенню критично важливі послуги. Більш того, вищі командири Збройних сил Сенти в Києві та посадові особи Військово-морських сил в Одесі та на острові Тотара отримали електронні листи з непідтверджених профілів з прямим попередженням «не виконувати накази політичного керівництва Сенти, інакше вони та їхні сім'ї будуть в небезпеці».

Соціальні мережі сповнені повідомлень і активних дискусій про можливе відділення південної частини Сенти. Ті ж новини поширюються через офіційні вебсторінки регіональних рад. Все вищевказане призводить до тиску та напруження всередині державних установ, правоохоронних органів і збройних сил. За останні 24 години різко посилилися вуличні демонстрації проти уряду Сенти, а саме в центральних містах південних регіонів: Одесі, Миколаєві та Херсоні. В результаті уряд функціонує на межі можливого, а населення збентежене.

На тлі значних кібератак, психологічного тиску, поширення дезінформації і дедалі більших вуличних протестів у південних регіонах на острові Тотара раптово висадилася значна кількість о/с збройних сил без розпізнавальних знаків. Доступ до порту острова Тотара заблокований вантажними суднами без розпізнавальних знаків і прапора держави. Доступ по воді до острова Тотара відрізаний. Бурові установки для видобутку вуглеводнів на острові Тотара, розташовані у ВЕЗ Сента, були захоплені й тепер знаходяться під повним контролем озброєних людей без розпізнавальних знаків.

Ввідна 4.5.1: День 56: 2 березня, 05:00

Озброєні люди без розпізнавальних знаків захопили вісім газових вишок біля острова Тотара у ВЕЗ Сенти. Вони висадилися на вишки за допомогою вертольотів і захопили їх. Військово-морські сили Бастана встановили зону контролю навколо бурових установок, а саме в районах Штормівського і Голіцинського газових родовищ. Цивільні судна й літаки повідомляють про значний збій у роботі GPS-сигналів в районі моря Нуар.

Реагування на Ввідну 4.5.1

На острові має бути встановлена військова присутність Сенти і посилені заходи для сил прикордонного патрулювання. Сента повинна негайно направити військових на острів через

проблеми з безпекою. Можна запровадити присутність спостережних, патрульних і дослідницьких кораблів, аби Румунія знала, чому Сента направляє туди війська.

Ввідна 4.5.2: День 58: 4 березня, 02:00

Минув місяць з моменту встановлення зони контролю у ВЕЗ Сенти, але контроль над морськими комунікаціями з боку Бастана триває. Значна кількість добре озброєних людей без розпізнавальних знаків і пробастанських активістів винаджуються на острів Тотара вночі за допомогою вертольотів і цивільних вантажних суден. Повідомлення про захоплення місцевих установ і основної військово-морської бази Сенти на острові. Для повного блокування доступу до військово-морської бази використовуються вантажні судна без розпізнавальних знаків і прапорів держави.



Реагування на Ввідну 4.5.2

У Сенти немає ефективного інструменту протидії агресії Бастана в Раді Безпеки ООН. Сента повинна забезпечити, аби міжнародна спільнота почула інформацію про реальну ситуацію, а не спотворену інформацію, надану Бастаном. Необхідні переговори на високому рівні. Невідомі озброєні люди та кораблі повинні бути ідентифіковані для запровадження санкцій.

Рекомендація: Для Сенти вкрай важливо продовжувати процес інформування міжнародної спільноти, аби всі знали правду про те, що відбувається. Постійний потік інформації повинен здійснюватися всіма можливими каналами, аби інформувати про ситуацію на весь світ.

Рекомендація: Принципи накладання санкцій повинні бути встановлені з регіональними, європейськими державами та державами-членами НАТО, аби забезпечити швидке введення жорстких і ефективних санкцій в подібних випадках, коли порушується територіальна цілісність. Санкції довели свою ефективність у минулому, але узгодження деталей того, що робити, часто відбувається занадто повільно.

7.5. Епізод 5: Посткризова стабілізація

Цей епізод присвячений посткризовому відновленню та процесу стабілізації. Посткризова стабілізація відбувається після закінчення кризового сценарію – з 7 березня 20XX року. Також потрібно обговорити питання управління в кризових ситуаціях.

Кожному синдикату буде запропоновано кілька питань для обговорення посткризової стабілізації.

1. Наскільки ефективною була реакція міжнародних організацій та міжнародної спільноти на маніпулювання Бастаном нормами міжнародного права в контексті захоплення/кібератаки на критичну інфраструктуру, виняткову морську економічну зону, морські торговельні шляхи та територію Сенти?
2. Чи мають міжнародні організації достатні важелі впливу в таких ситуаціях?
3. Чи повинні міжнародні санкції проти Бастана поширюватися тільки на його організації (установи), окремих осіб, безпосередньо залучених до кризи, і не поширюватися на всю країну? Якими можуть бути механізми для міжнародної спільноти щодо введення таких санкцій і контролю над їх дотриманням?
4. Які заходи слід застосувати до країни, яка ігнорує міжнародне право?

Відповіді на запитання

Введення санкцій щодо компаній, причетних до анексії півострова Сенти, в минулому було досить ефективним для міжнародних організацій, але Сенті знадобилося дуже багато часу, аби ввести їх в дію. Важливо зібрати офіційну інформацію, яка може повністю підтримати судові позови проти цих компаній, оскільки чинне законодавство Сенти не регулює це питання. РНБО рухається в цьому напрямку.

Що стосується введення санкцій щодо Бастана, то є кілька варіантів, які залежать від того, чи є вони санкціями Сенти або міжнародними санкціями. Ефективність цих санкцій різна. Негативом є те, що ООН або не вводить санкції, які були прийняті, або пропонує їх введення, але вони постійно блокуються. Сенті необхідно визначити, від кого вона може отримати підтримку щодо введення подальших санкцій. Наприклад, США і ЄС можуть підтримати своєю власною заборонаю на купівлю військової техніки у Бастана, це третє за величиною джерело доходу для них.

Може бути введено ефективне ембарго на експорт енергетичних продуктів олігархів, а також накладено арешт на активи бастанських олігархів. Санкції проти суб'єктів, які видобувають газ з бурових установок у морі Нуар, не повинні допускати продажу такого газу на міжнародному рівні. Сента споживає 80% палива з Бастана. У Сенті є тільки один нафтопереробний завод з низьким рівнем завантаження через імпорту з Бастана. Сенті необхідно змінити свої принципи щодо імпорту нафти, аби сприяти збільшенню використання місцевого продукту. Це велика проблема, як зробити санкції ефективними.

Коли починаються масові заворушення, Головнокомандувач віддає наказ кораблям почати рух в проблемну зону. Чи можемо ми звернутися за допомогою до Румунії? Чи можемо ми звернутися до наших держав-партнерів з проханням про гуманітарну допомогу у вигляді дизельного палива для наших суден і гуманітарної допомоги у вигляді постачання палива? Непросте завдання для вирішення, коли є питання, що залишилися без відповіді.

Ми повинні мати на увазі, що у випадку, якщо Одеса буде окупована сепаратистами, що ми будемо робити далі? Окрім санкцій, у нас є деякі механізми НАТО, які ми можемо використовувати. На кого ще ми можемо покластися в допомозі? Чого від них можна очікувати? Є деякі сфери поза межами СТРАТКОМ, впливові люди, які є лідерами громадської думки. Чи є у МЗС певний список і постійна співпраця? Робота з лідерами опозиції Бастана, аби збільшити допомогу.

Нуарморська робоча група збирається з різних країн, вони діляться своїм досвідом. Є також групи юристів, які підтримують ці справи. Як вони спілкуються з населенням? Наші навчальні центри повинні використовуватися для висвітлення обставин, що мали місце, і всіх юридичних наслідків того, що було зроблено і які закони були порушені. Забезпечення широкого інформування суспільства.

Є Парламентська асамблея НАТО і міжпарламентська рада. Ефективна робота з міжнародною спільнотою повинна початися з першого дня. Це повинно відбуватися на найперших етапах, до захоплення суден тощо.

Рекомендація: у випадку гібридної війни Сента повинна впевнено робити й надсилати багатосторонні міжнародні прохання про допомогу, а не застрягати в очікуванні прийняття рішень органами, які працюють повільно. Сента повинна мати можливість просити та отримувати допомогу на багатосторонній основі, швидко і без вагань.

7.6. Ключові висновки

* Читачі повинні пам'ятати, що цей Синдикат включив кілька рекомендацій у свої відповіді на конкретні епізоди/ввідні, які не включені в ключові висновки.

Реакція міжнародних партнерів Є необхідність в індивідуальних рішеннях для протидії загрозам, пов'язаним з політичними, правовими, економічними та енергетичними проблемами. Потрібні національні та міжнародні правові акти, що стосуються захисту критичної інфраструктури та питань енергетичної безпеки на високому рівні. Також необхідні негайні дії для сприяння належному реагуванню президента та уряду щодо координації дій з міжнародними партнерами для протидії конфліктним ситуаціям. **Рекомендація:** Рекомендовано відновити та модифікувати спільну робочу групу Україна-НАТО з економічної безпеки. Потрібне оновлення законодавства України, що має бути здійснене відповідно до Угоди про асоціацію між Україною та ЄС. Це зміцнить енергетичну незалежність країни під час кризи шляхом забезпечення мінімальних запасів нафти і нафтопродуктів; створення страхових резервів газу (відповідно до рекомендацій ЄС) і вдосконалення правової бази для зміцнення транскордонних відносин і співробітництва. Підтримати збільшення місцевого видобутку вуглеводнів, газу і нафти поряд з розвитком нафтопереробної галузі та нафтохімії. Прийняти правила ЄС в Україні для інфраструктурних проєктів, а також для розгортання інфраструктури для альтернативних і зневоднених видів палива. Залучити депутатів українського

парламенту до ініціювання запитів до парламентів інших держав, а також використовувати можливості Парламентської асамблеї НАТО.

Міжнародні угоди Вимагати дотримання сторонами зобов'язань за юридичними угодами та будь-якими можливими поправками. Оновлення міжнародних договорів створить основу для використання міжнародної судової системи у разі конфлікту. **Рекомендація:** Переглянути вже наявні міжнародні угоди (наприклад, Будапештський меморандум, Конвенцію Організації Об'єднаних Націй з морського права, Статут Чорноморського Економічного Співробітництва). Оцінити всі міжнародні угоди, що стосуються українського прикордонного співробітництва; зокрема, екологічну та військову взаємодію, а також взаємодію у випадку надзвичайних ситуацій під час кризи. Покращити технічні спроможності для обміну розвідувальною інформацією з використанням Партнерства розширених можливостей. Залучати громадянське суспільство та фахівців/експертів для підвищення міжнародної обізнаності та просування позицій України, посилюючи систематичну взаємодію з особами, які формують громадську думку, та особами, які приймають рішення в державах-партнерах. Створити національну базу даних про порушення міжнародних договорів, засновану на фактичних даних, з акцентом на райони з високим рівнем конфліктів.

Внутрішня готовність до міжнародного співробітництва Потрібна адаптація деяких найбільш актуальних національних документів до викликів, пов'язаних з питаннями енергетичної безпеки, аби полегшити процес формування юридично зобов'язальної основи для консолідованого міжнародного реагування. Це дозволить уникнути порушень національного законодавства, створивши сприятливе і продуктивне середовище для розвитку міжнародних відносин. **Рекомендація:** Розвиток Україною міжрегіонального співробітництва надзвичайно важливий на початку конфлікту, аби уникнути створення умов для ескалації. Створити мережу філіалів центрів ситуативної обізнаності для покращення співпраці між українськими державними органами у разі кризи. Розробити Національний план дій щодо забезпечення безпеки на морі та налагодити співпрацю між Міністерством закордонних справ (МЗС) та Службою зовнішньої розвідки України для негайного обміну інформацією та підвищення готовності. Створити механізм запиту інформації між державними органами України та МЗС щодо їх потреб від міжнародних організацій, аби уникнути дублювання зусиль та забезпечити належну координацію. Розробити відповідні скоординовані дії для прогнозування та протидії енергетичним загрозам щодо України, Європейського Союзу та інших країн регіону. Проводити міжнародні навчання між підрозділами Збройних сил України, Національної гвардії України, Національної поліції України та Державної прикордонної служби України з відповідними підрозділами іноземних держав.

8. Підсумки

CORE 20 були навчаннями національного рівня, спрямованими на підвищення стійкості систем критичної інфраструктури України за допомогою міжвідомчої участі на високому рівні. Цей захід послужив найважливішою платформою для співпраці з більш ніж 150 учасниками з 15 країн і більш ніж 50 організацій. Серія презентацій і робіт синдикатів була інформативною і корисною для виявлення прогалин у стійкості критичної інфраструктури, стратегій зниження ризиків, передового досвіду та рекомендацій для застосування Урядом України.

Нижче наведені ті ключові висновки й рекомендації – деякі з яких були представлені в день високоповажних гостей/під час обговорення результатів – що були визначені розширеним складом команд, що склалися з координаторів, учасників й оцінювачів, які разом працювали над поданими звітами синдикатів, об'єднаними в главах цього звіту, з темами, які виходять за рамки конкретних пріоритетних напрямків аналізу синдикату.



Під час засідання в день високоповажних гостей Ольга Стефанішина, Віцепрем'єр-міністр з питань європейської та євроатлантичної інтеграції, виступила з промовою, де відзначила важливість КШН НАТО CORE20 для підвищення стійкості України.

8.1. Ключові висновки та рекомендації, підбиваючи підсумки проведеного навчання

Напрямки для покращення роботи

Економічна стійкість вимагає більшої уваги. Зараз основна увага в забезпеченні стійкості робиться на фізичну безпеку інфраструктури та захист енергетичних систем. А те що залишається, то це інші ризики, такі як дефіцит постачання енергоносіїв через політичні ризики. Необхідно мати достатнє та безперервне постачання енергоресурсів, аби системи могли функціонувати. Для захисту від перебоїв

в постачанні потрібна більша різноманітність джерел енергії та її зберігання. Стійкість сама по собі не гарантує постачання. **Рекомендація:** Паливо та інші життєво важливі предмети постачання (продовольство, вода, критично важливі матеріали) вимагають адекватних рівнів зберігання, заснованих на циклах і функціонуванні ланцюжка постачання.

Брак технічно кваліфікованого персоналу. Занадто часто навчений і досвідчений персонал виїжджає за кордон, створюючи критичну нестачу необхідних технічних фахівців і досвіду для підтримки стійкості. Стандартне повідомлення про звільнення становить чотири тижні. Цього часу недостатньо для заміни такого кваліфікованого персоналу. **Рекомендація:** Розглянути можливість укладання довгострокових контрактів з технічно кваліфікованим персоналом, відповідальним за критичну інфраструктуру, та розглянути інші заходи щодо обмеження такого «витоку мізків» через налагодження партнерських відносин між урядом, представниками галузі та академічними колами, що має призвести до створення робочих місць та позитивного результату від цього.

Міжвідомча співпраця на рівні нижче міністерства. Кожна урядова установа нижче міністерського рівня усвідомлює свої власні функції та обов'язки й володіє відповідними спроможностями, і кожна діє самостійно, ґрунтуючись на вказівках міністерства, а не узгоджено з іншими установами в рамках свого міністерства або за його межами. Учасники визнали необхідність розширення міжвідомчої співпраці для найкращого забезпечення стійкості критичної інфраструктури та енергетичних систем. Не існує формального регуляторного механізму для визначення процесів того, як має відбуватися така взаємодія. **Рекомендація:** Необхідно розробити офіційні міжвідомчі механізми для формалізації міжвідомчого співробітництва. Після їх розробки персонал департаменту також потребує навчання практичним аспектам ведення таких комунікацій і зв'язків. Така взаємодія повинна здійснюватися на кожному рівні, між установами й регіонами, а також на об'єктах критичної інфраструктури, наприклад в порту.



Під час засідання в день високоповажних гостей полковник Даріус УЖКУРАЙТІС, директор Центру передового досвіду НАТО в галузі енергетичної безпеки, представляє загальний огляд КШН НАТО CORE 20 в Одесі, Україна.

Визначення критичної інфраструктури. Всіма українськими відомствами не було погоджене жодне універсальне офіційне визначення «критичної інфраструктури». Як тимчасовий захід Служба безпеки (СБУ) склала власний список об'єктів критичної інфраструктури, який не був переданий іншим відомствам. Оскільки законодавчого визначення цього терміну не існує, подальше укомплектування персоналом, координація та оцінка не проводяться. **Рекомендація:** Визначити провідну установу для підтримки прийняття необхідних законів і законодавчих актів, які дозволять створити стійкі системи. Національний парламентський комітет все ще перебуває в процесі розгляду цієї резолюції. В цей час на розгляді Кабінету Міністрів знаходиться постанова про визначення об'єктів критичної інфраструктури. У міністерствах мало експертів, які могли б зосередитися на цих питаннях, і в цьому процесі їм може знадобитися зовнішня підтримка.

Вимога про закриття можливих в перспективі стиків між національними підрозділами по забезпеченню стійкості. У результаті одночасних і послідовних нетрадиційних методів були задіяні бастанські та неідентифіковані озброєні люди для створення конфліктних і кризових ситуацій, процес прийняття рішень на національному, регіональному та місцевому рівнях був непослідовним, а застосовна правова база і регулювання для національної та регіональної координації між відомствами/органами були непрозорими. **Рекомендація:** Підвищити готовність національних підрозділів по забезпеченню стійкості шляхом впровадження системи раннього включення та широкої взаємодії всіх підрозділів стосовно гібридних загроз, аби передача відповідальності між підрозділами мала меншу кількість прогалин/проблем щодо наступності.

Вирішити/усунути невизначеність організаційної моделі забезпечення національної стійкості.

Об'єднана/єдина методологія оцінки ризиків для національної безпеки та стану відповідних спроможностей для підготовки, прийняття та реалізації рішень часто обговорювалася Збройними Силами, Радою національної безпеки і оборони та Антитерористичним центром Сенти. **Рекомендація:** Забезпечити реалізацію стратегічного документа у сфері морської безпеки, який, зокрема, визначатиме основи захисту національних інтересів на морі та впровадження системи управління ризиками, зокрема, їх оцінки, та розробки заходів щодо мінімізації їх впливу.



Під час засідання в день високоповажних гостей учасники та координатори заслухали доповіді синдикатів.

Передовий досвід/Сильні сторони

Комунікація в кризових ситуаціях. Державна служба спеціального зв'язку України є незалежним агентством/службою, яка ефективно забезпечує комунікацію в кризових ситуаціях для всіх відомств, регіонів та об'єктів, а також відповідає за аспекти стратегічних комунікацій. Національний центр телекомунікацій та спеціального зв'язку надає лінії екстреного зв'язку між усіма відомствами й забезпечує функціональне оперативне управління на рівні уряду. Система зв'язку не може бути зламаною, зазнати втручання, пошкодженою або відключеною. **Рекомендація:** Цей ефективний, контрольований і фінансований державою національний апарат зв'язку слід розглянути для країн-партнерів, у яких може не бути такої надійної системи.

Розуміння і зменшення наслідків російських кампаній з дезінформації. Російська кампанія з дезінформації була ефективною в поширенні неправдивої інформації, створенні розбіжностей і підриві довіри до здатності режиму, щодо якого націлена кампанія, правити й управляти. Однак за останні кілька років Україна отримала багато практичного досвіду щодо зменшення наслідків і протидії російській дезінформації, зокрема, її успіхи в зміцненні довіри населення, спростуванні фальшивої пропаганди, і сьогодні велика частина населення України може відрізнити фейки від справжньої інформації. Тому в Росії зараз немає можливості змінити думку України; є деякі проросійські налаштовані українці, які, незважаючи ні на що, підтримають російську дезінформацію. **Рекомендація:** Спроможності України з протидії російським кампаніям з дезінформації вигідні іншим країнам, які стикаються з аналогічними загрозами.

Зміцнена рішучість населення. Україна визнала, що в часи кризи, коли розтягуються сили безпеки у відповідь на великі інциденти та операції, населення не прагне отримати вигоди через мародерство і злочинну діяльність. У цьому сенсі спроба Росії послабити Україну зміцнила рішучість багатьох українців піти на жертви, аби зберегти суверенітет України та виступити проти ворожих дій Росії.



Під час засідання в день високоповажних гостей представник урядового офісу, полковник Сергій ВЕРБИЦЬКИЙ виступає з вітальним словом в Одесі, Україна.

8.2. Закриття навчань

Важливо відзначити, що цей звіт, в ідеалі, не завершує навчання CORE 20, оскільки міністерства та організації України, які брали участь у КШН, повинні розробити План підвищення ефективності діяльності на основі відповідних окреслених ключових висновків. Кожна установа повинна додатково проаналізувати ключові висновки, що стосуються її організацій, аби визначити найкращі засоби для сприяння поліпшенням і розробки відповідного плану дій для внесення таких позитивних змін з метою підвищення ефективності та результативності реагування її організацій на виклики, пов'язані з критичною енергетичною інфраструктурою, й гібридні загрози – такий продукт становитиме її План підвищення ефективності діяльності. Крім того, Центр передового досвіду НАТО в галузі енергетичної безпеки ENSEC COE розробив проєкт щодо звернення до учасників CORE в різні моменти в майбутньому (через шість місяців, один рік тощо), аби провести опитування учасників про будь-які поліпшення, реалізовані на основі того, що було засвоєно під час CORE 20. Після КШН CORE20 27 вересня 2021 року був підписаний Указ Президента «Про Концепцію забезпечення національної системи стійкості», 16 листопада 2021 року набув чинності Закон «Про критичну інфраструктуру», а 11 лютого 2022 року Рада національної безпеки і оборони України затвердила Стратегію морської безпеки України.



СПІЛЬНЕ ФОТО УЧАСНИКІВ CORE 20.

Додатки

Список організацій-учасниць

- Штаб-квартира НАТО
- Командування ОЗС НАТО з питань трансформації
- Центр передового досвіду НАТО в галузі енергетичної безпеки
- Центр передового досвіду НАТО в галузі морської безпеки
- Центр передового досвіду НАТО в галузі стратегічних комунікацій
- Центр передового досвіду спільного кіберзахисту НАТО
- Командування сил спеціальних операцій НАТО
- Представництво НАТО в Україні
- Центр боротьби з гібридними загрозами
- Школа післядипломної освіти ВМС США
- Національний інститут стратегічних досліджень України
- Національний університет оборони України імені Івана Черняховського
- Центр інформації та документації НАТО
- Посольство Канади
- Посольство Республіки Молдова в Україні
- Посольство Республіки Болгарія в Україні
- Посольство Королівства Данія в Україні
- Посольство Естонської Республіки в Україні
- Посольство Республіки Фінляндія в Україні
- Посольство Грузії в Україні
- Посольство Федеративної Республіки Німеччина в Україні
- Посольство Японії в Україні
- Посольство Литовської Республіки в Україні
- Посольство Республіки Молдова в Україні
- Посольство Королівства Норвегія в Україні
- Посольство Румунії в Україні
- Посольство Республіки Словаччина в Україні
- Посольство Королівства Швеції в Україні
- Посольство Республіки Туреччина в Україні
- Посольство Сполученого Королівства Великої Британії і Північної Ірландії в Україні
- Посольство Сполучених Штатів Америки в Україні
- Рада національної безпеки і оборони України
- Служба безпеки України
- Міністерство внутрішніх справ України
- Міністерство оборони України
- Міністерство економіки України
- Міністерство інфраструктури України
- Міністерство закордонних справ України
- Міністерство юстиції України
- Збройні Сили України

- Військово-морські сили України
- Державна служба спеціального зв'язку та захисту інформації України
- Державна служба України з надзвичайних ситуацій
- Національна поліція України
- Національна гвардія України
- Одеська обласна державна адміністрація
- НАФТОГАЗ
- УКРЕНЕРГО
- Оператор ГТС України
- Укрзалізниця (Одеське відділення)
- Офіс Президента України
- Національний координаційний центр кібербезпеки України
- Міністерство культури та інформаційної політики України
- Державна прикордонна служба України
- Державний комітет телебачення і радіомовлення України
- Місія України при НАТО
- ГО «Українська призма»
- Адміністрація морських портів України
- Національний банк України
- Урядовий офіс координації європейської та євроатлантичної інтеграції

Результати опитування учасників щодо оцінки навчань

Оцінка командно-штабних навчань CORE 20: аналіз коментарів за результатами опитування учасників щодо оцінки навчань

Оцінка учасників (Додаток 3) під час КШН показує, що більшість учасників відзначили цей тип заходу як дуже корисний – переважна більшість заявила, що аспект «найбільше сподобалося» в навчаннях – це можливість взаємодіяти та вести діалог з іншими відомствами та іноземними партнерами. Багато учасників також відзначили, що їм сподобалися сценарії, вибрані для навчань, особливо через їх реалістичність і застосовність до реальних сценаріїв. У кількох коментарях йшлося про високий рівень організації командно-штабних навчань, дискусій і презентацій.

Коли учасникам було запропоновано описати, що їм найменше сподобалося під час КШН CORE, то велика кількість учасників вказали, як їм не сподобалося те, що вони не могли взаємодіяти з іншими синдикатами під час обговорень. Кілька учасників вказали, що було мало часу для обговорення сценаріїв, епізодів і ввідних. Однією з можливих причин браку часу для обговорень було названо те, що багато часу займав переклад. Іншою причиною, на яку вказують деякі учасники, могла бути «постійна зміна формату презентацій».

Коли їх попросили висловити пропозиції щодо того, як можна поліпшити КШН CORE, то велика кількість учасників запропонували структурні зміни в синдикатах. Пропозиції включали таке: 1) «створити ще один синдикат, який охоплював би всі інші синдикати, [із загальною метою] провести остаточну оцінку; 2) зменшити кількість синдикатів, аби створити більш ефективні, компактні групи з участю як військових, так і цивільних представників; 3) проводити командно-штабні навчання на регулярній основі та запрошувати більше експертів з інших відомств, таких як Міністерство охорони здоров'я і Міністерство інфраструктури, і 4) все для того, аби синдикати взаємодіяли та вели діалог один з одним під час навчань.

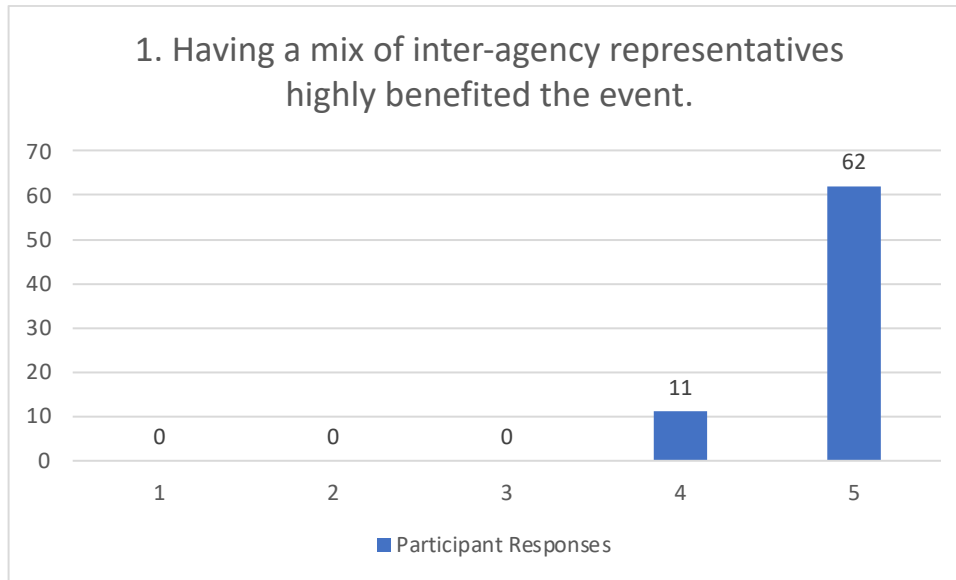
Аналогічним чином, багато пропозицій стосувалися відточування практичності та застосовності сценаріїв. Наприклад, було внесено кілька пропозицій, аби більше «практичних» завдань було зосереджено на кібербезпеці, технічних випадках і прикладах, пов'язаних з організаційною роботою.

Багато учасників також запропонували виділити більше часу для обговорення та аналізу епізодів і надати керівникам груп 20-30 хвилин на доопрацювання плану дій щодо епізодів. Були також висловлені пропозиції «краще інформувати» учасників про цілі та завдання, очікувані від них під час навчань, перш ніж вони розпочнуться.

Результати опитувань учасників щодо оцінки навчань

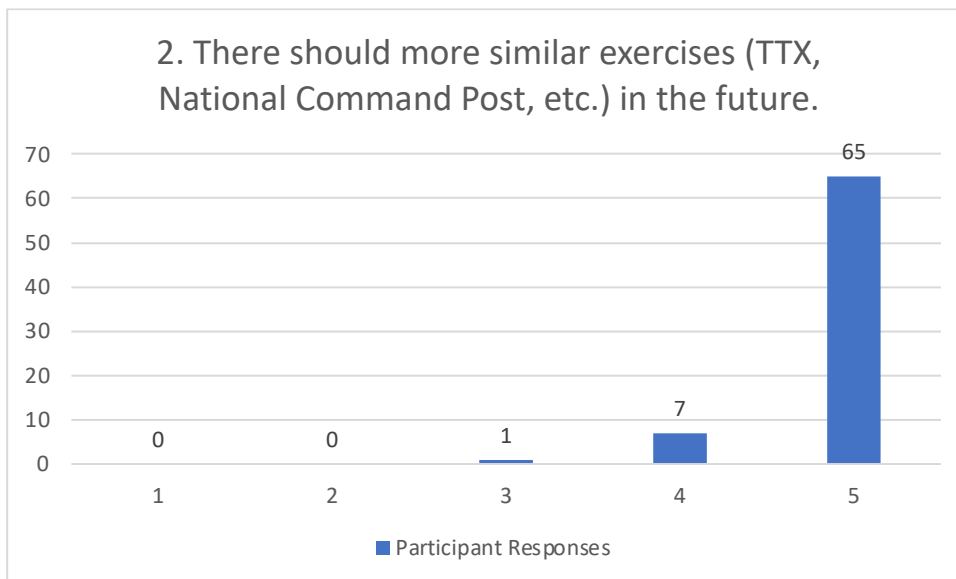
Кількісна оцінка Частина I

❖ Будь ласка, дайте відповідь на вказані нижче питання/твердження за шкалою від 1 до 5, де 1 означає «КАТЕГОРИЧНО НЕ ЗГОДЕН», а 5 - «ПОВНІСТЮ ЗГОДЕН»:



1. Присутність представників різних відомств була вкрай корисною для Заходу.

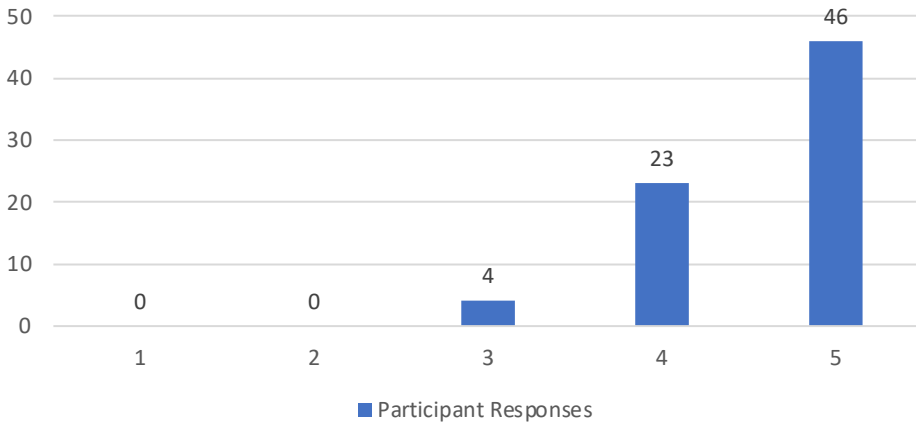
■ Відповіді учасників



2. Необхідна більша кількість подібних навчань у майбутньому (КШН, Національний командний пункт тощо).

■ Відповіді учасників

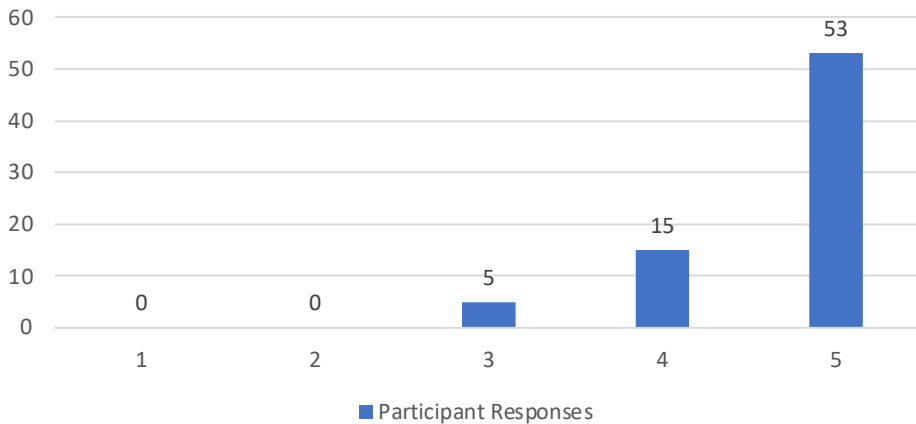
3. My participation in CORE TTX was very beneficial for my current job duties.



3. Моя участь у КШН CORE була дуже корисною для моїх поточних функціональних обов'язків

■ Відповіді учасників

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

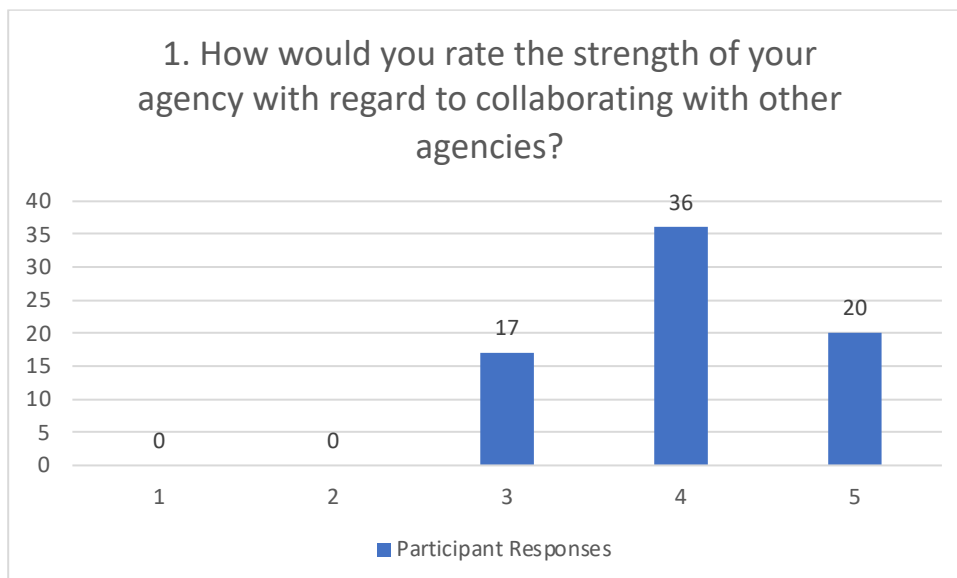


4. Участь у КШН CORE була б дуже корисною для моїх колег, якби вони мали змогу відвідати їх

■ Відповіді учасників

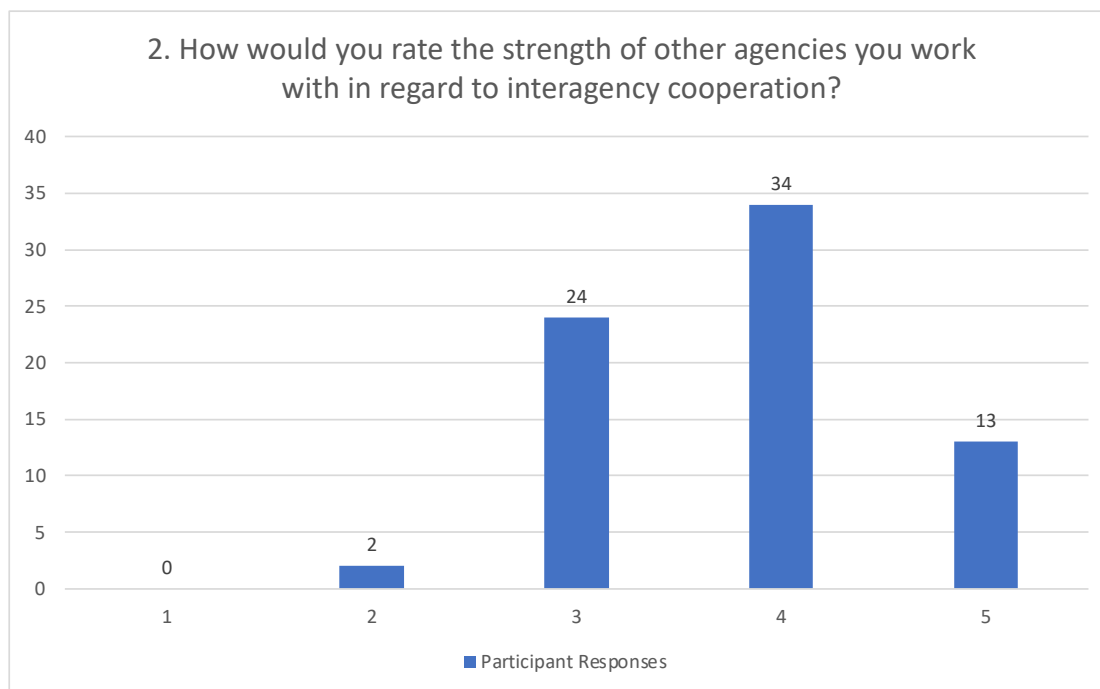
Кількісна оцінка Частина 2

❖ Будь ласка, дайте відповідь на вказані нижче питання за шкалою від 1 до 5, де 1 означає «ПОТРЕБУЄ ЗНАЧНОГО ПОЛІПШЕННЯ/КАТЕГОРИЧНО НЕ ЗГОДЕН», а 5 – «ДУЖЕ ДОБРЕ/ПОВНІСТЮ ЗГОДЕН»:



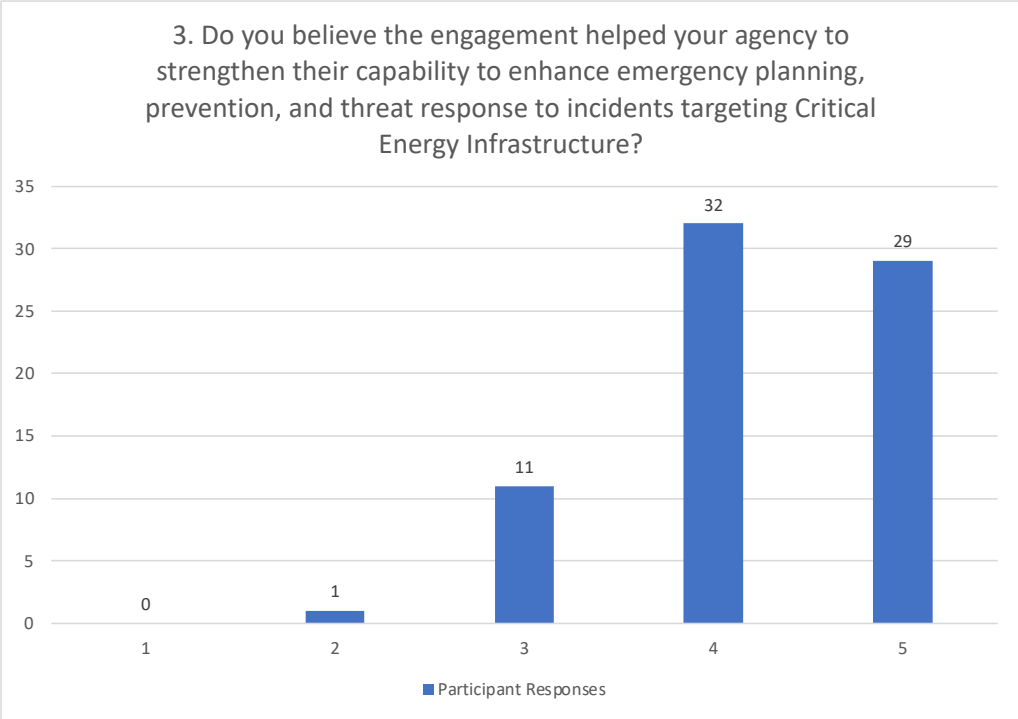
1. Як би ви оцінили ефективність вашого відомства стосовно співпраці з іншими відомствами?

■ Відповіді учасників



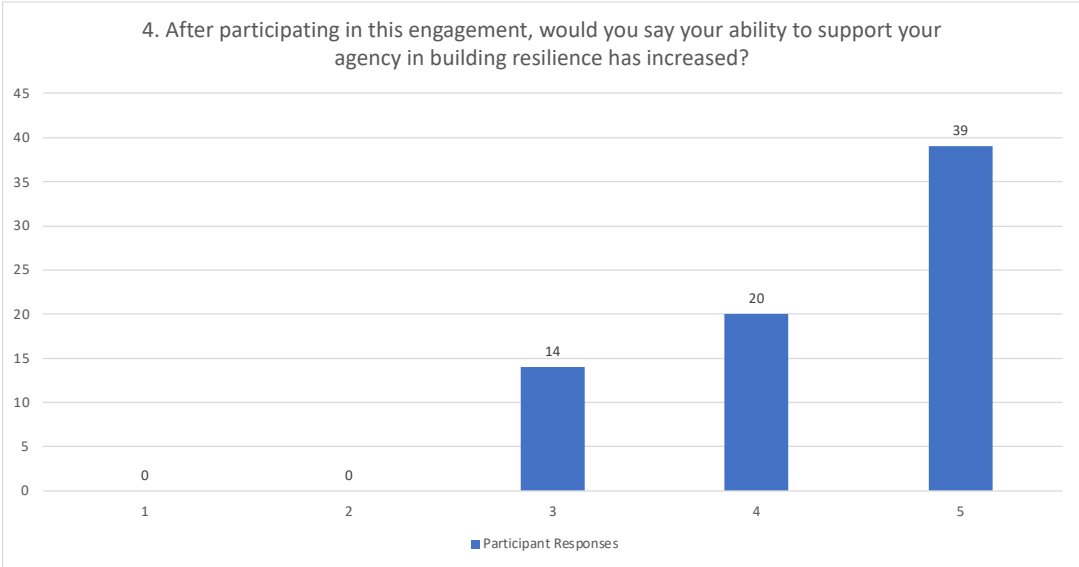
2. Як би ви оцінили ефективність інших відомств, з якими ви працюєте, стосовно міжвідомчої співпраці?

■ Відповіді учасників



3. Чи вважаєте ви, що залучення допомогло вашому відомству зміцнити спроможності для покращення планування на випадок надзвичайних ситуацій, запобігання й реагування на загрози у випадку інцидентів на критичну енергетичну інфраструктуру?

■ Відповіді учасників



4. Після участі у заході чи можете ви сказати, що посилились ваші навички щодо підтримки вашого відомства у розбудові системи стійкості?

■ Відповіді учасників

Глосарій скорочень

Скорочення	Визначення
ПП	Підбивання підсумків
КЕІ	Критична енергетична інфраструктура
АСУ	Автоматизовані системи управління
ППЕД	План підвищення ефективності діяльності
НД	Незалежне дослідження
ІТ	Інформаційна технологія
АЕС	Атомна електростанція
кВ	Кіловольт(и).
ГВт	Гігаватт
SCADA	Система диспетчерського управління та збору даних
КШН	Командно-штабні навчання
ОЕС	Об'єднана енергетична система

Глосарій термінів

Термін	Визначення
Кінцевий звіт про навчання	Підсумковий звіт про навчання (ПЗН) – це кінцевий продукт навчань. Підсумковий звіт про навчання/План підвищення ефективності діяльності (ПЗН/ППЕД) складається з двох компонентів: ПЗН, в якому фіксуються зауваження та рекомендації, засновані на основних цілях навчань, і План підвищення ефективності діяльності (ППЕД), який визначає конкретні коригувальні дії, призначає відповідальних і встановлює цільові показники для їх виконання.
Спроможність	Засіб виконання одного або декількох завдань в певних умовах з метою дотримання певних стандартів ефективності, для досягнення наміченого.
Критична інфраструктура	Сукупність об'єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості, функціонування суспільства і безпеки населення, і виведення з експлуатації або руйнування яких може вплинути на національну безпеку та оборону, довкілля, призвести до значних фінансових втрат і людських жертв
Кібератака	Несанкціоновані дії, що здійснюються з використанням інформаційно-комунікаційних технологій і спрямовані на порушення конфіденційності, цілісності та доступності інформації, оброблюваної в інформаційно-телекомунікаційній системі, або порушення сталого функціонування такої системи;
Критична інфраструктура	Підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінансова система, інформаційні технології та телекомунікації (електронні комунікації), харчові продукти, охорона здоров'я, комунальні послуги, які стратегічно важливі для функціонування економіки та безпеки держави, суспільства і населення.
Кіберпростір	Глобальна сфера в інформаційному середовищі, що складається з взаємозалежної мережі інфраструктури інформаційних систем, у тому числі Інтернет, телекомунікаційні мережі, комп'ютерні системи, вбудовані процесори

Термін	Визначення
Диверсія	Вчинення з метою ослаблення держави вибухів, підпалів або інших дій, спрямованих на масове знищення людей, заподіяння тілесних ушкоджень або іншої шкоди їх здоров'ю, знищення або пошкодження об'єктів, що мають істотне економічне або оборонне значення, а також вчинення з цією метою дій, спрямованих на радіоактивне зараження, масове отруєння, поширення
Безпека електропостачання	Здатність електроенергетики забезпечувати потреби споживачів в електричній енергії відповідно до вимог законодавства
Відповідальний за збір даних	Персонал навчань, відібраний з різних установ для оцінки та надання коментарів у певних функціональних сферах знань; також згадується як «Спостерігач»
Доповідь по завершенню	Збори планувальників, координаторів і оцінювачів для проведення аналізу та надання відгуків під час направленої обговорення після проведення навчань.
Навчання	Імітаційна діяльність, що проводиться для тренування однієї операції, структури управління або організації; надає можливості для тестування планів і підвищення майстерності реагування в умовах відсутності ризиків
Графік виконання навчань	Визначає планувальні конференції та завдання, необхідні для планування і розробки навчань
Направлене обговорення	Цілеспрямоване обговорення конкретних питань за допомогою Координатора, що має досвід у функціональній області або є предметним експертом.
Обговорення результатів	Направлене обговорення, що проводиться відразу після навчань між учасниками навчань з кожної функціональної області. Призначене для збору відгуків про будь-які питання, проблеми або пропонувані поліпшення, які можуть виникнути в учасників стосовно навчань. Оцінювачі також можуть запитати про роз'яснення щодо певних дій і того, що спонукало учасників їх зробити.
План підвищення ефективності діяльності	Група з однієї або декількох рекомендацій і переліку заходів, визначених для усунення недоліків, виявлених під час події; для кожного завдання в ППЕД перераховані коригувальні дії, які будуть зроблені, відповідальна сторона або відомство й очікувана дата завершення; знаходиться в кінці ПЗН

Термін	Визначення
Морська безпека	Міжнародна та міжвідомча, цивільна та військова діяльність щодо зниження ризику та протидії незаконній або загрозовій діяльності в морській сфері, з метою застосування заходів впливу на них для забезпечення дотримання закону, захисту громадян і захисту національних і міжнародних інтересів. Таким чином, морська безпека буде зосереджена на незаконному використанні морського простору.
Операції з морської безпеки	Дії, що здійснюються на морі тими військовими й цивільними органами влади, які оснащені відповідними засобами та уповноважені реагувати на ризики й загрози, пов'язані з морською безпекою.
Дискусія з модератором	Направлена форма обговорення, в якій представник кожної функціональної області представляє учасникам резюме і результати з попереднього направлено обговорення групи.
Спостереження	Дія з реєстрації даних під час навчання
Оцінювач	Персонал навчань, відібраний з різних установ для оцінки та надання коментарів у певних функціональних сферах знань; також згадується як «Відповідальний за збір даних»
Аналіз	Оцінка областей, в яких організація працює дуже добре, і областей, які потребують поліпшення
Об'єкт електроенергетики	Електростанція (на додаток до ядерного обладнання атомної електростанції), електрична підстанція, електрична мережа
Група планування/ Член групи контролю навчань	Будь-який персонал, який виконує роль або завдання у складі Групи планування навчань
Управління проєктом	Координація персоналу, ресурсів і стратегічних цілей для окремої справи в рамках навчань
Електростанція	Електроустановка або група електроустановок, призначених для виробництва електричної енергії або комбінованого виробництва електричної та теплової енергії
Реальна подія	Фактичний інцидент, що матеріалізує загрозу життю, майну, населенню та довкіллю
Рекомендація	Визначення областей для поліпшення, визначених під час навчань або отриманих як досвід під час реальних подій; на основі аналізу першопричин рекомендації перераховані у всіх ПЗН/ППЕД

Термін	Визначення
Терористичний акт	Застосування зброї, вчинення вибуху, підпалу або інших дій, які створили небезпеку для життя або здоров'я людини, або завдали значної матеріальної шкоди або інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту, ускладнення міжнародної ситуації, або з метою вплинути на прийняття рішень або на вчинення чи не вчинення дій органами державної влади або місцевого самоврядування, службовими особами цих органів, юридичними особами, або привернення уваги громадськості до певних політичних, релігійних або інших поглядів злочинця (терориста), а також погроза вчинення цих дій для цих же цілей.
Вразливість	Фізична особливість або експлуатаційний атрибут, який робить об'єкт, актив, систему, мережу або географічну область відкритими для експлуатації або схильними до певної небезпеки
Об'єднана енергетична система (ОЕС Сенти)	Сукупність електростанцій, електричних мереж, інших об'єктів електроенергетики, об'єднаних загальним режимом виробництва, передачі та розподілу електричної енергії з централізованим управлінням цим режимом



Це пам'ятник «Золоте дитя», що знаходиться в Одеському порту за межами місця проведення КШН CORE 20.