НЕВОЄННИЙ ВИМІР ВІЙН НОВОГО ПОКОЛІННЯ: ЕНЕРГЕТИЧНИЙ КОМПОНЕНТ

КИЇВ 2016

Упорядники:
Бобро Д.Г., провідний науковий співробітник відділу енергетичної та техногенної безпеки НІСД, к. ф.-м. н.
Синиця С. Л., керівник проекту, Київський міжнародний енергетичний клуб
Під загальною редакцією Гончара М. М., президента Центру глобалістики «Стратегія XXI» та Суходолі О.М. завідувача відділу енергетичної та техногенної безпеки НІСД, д.держ.упр., професора

Невоєнний вимір війн нового покоління. Енергетичний компонент
Матеріали за підсумками міжнародної конференції

Електронна версія: http://niss.gov.ua http://geostrategy.org.ua http://qclub.org.ua

Брошура містить матеріали міжнародної конференції «Невоєнний вимір війн нового покоління. Енергетичний компонент», що була організована Національним інститутом стратегічних досліджень, Центром глобалістики «Стратегія XXI» та Центром передового досвіду НАТО з питань енергетичної безпеки 17 березня 2016 року у м. Києві. Конференція відбулась за фінансової підтримки Міжнародного фонду «Відродження» та організаційного сприяння Київського міжнародного енергетичного клубу «Q-клуб».

За підтримки:

міжнародний фонд Відродження INTERNATIONAL RENAISSANCE FOUNDATION

Q Club energy Kyiv International Energy Club

Зміст:

Про конференцію.

17 березня 2016 року в Національному інституті стратегічних досліджень відбулася Міжнародна конференція «Невоєнний вимір війн нового покоління. Енергетичний компонент»

Захід організований НІСД спільно з Центром передового досвіду НАТО з питань енергетичної безпеки (м. Вільнюс, Литва) та Центром глобалістики «Стратегія XXI» (м. Київ, Україна). У конференції взяли участь представники органів державної влади, правоохоронних органів, інститутів НАНУ, вищих навчальних та профільних науково-дослідних закладів, а також провідних компаній паливно-енергетичного комплексу (список учасників).

У вступному слові перший заступник директора Інституту **Олександр Власюк** привітав учасників конференції та зазначив, що для України питання функціонування національного енергетичного сектору в умовах гібридної війни – питання не теорії, а практики, і в Україні готові як поділитися набутим досвідом, так і з вдячністю сприйняти досвід зарубіжних партнерів щодо захисту критичної енергетичної інфраструктури.

Олександр Власюк зазначив, що нині Україна живе в умовах гібридної війни з Росією, а російська агресія є довгостроковим чинником впливу на українську внутрішню та зовнішню політику. При цьому унікальність ситуації полягає в узгодженості та взаємозв'язку різних елементів, які використовуються російською стороною в розв'язаній нею гібридній війні, динамічності та гнучкості їх застосування, а також колосального зростання важливості інформаційного чинника. Він наголосив, що геополітичним змістом російської зовнішньої політики було і є унеможливлення становлення української незалежної держави, а для реалізації цієї стратегії Кремль створив комплексну систему політико-дипломатичного, економічного, насамперед енергетичного, інформаційно-пропагандистського та воєнного тиску на Україну.

Доповідач підкреслив, що важливим елементом у російській гібридній війні стала російська енергетична політика, використання якої як інструменту політики було проголошено Росією ще у 2003 році в Енергетичній стратегії Російської Федерації до 2020 року, де було зазначено, що паливно-енергетичний комплекс Росії є «інструментом здійснення внутрішньої та зовнішньої політики». Остаточно ж російський інструмент енергетичного тиску на Україну був сформований у 2009 році після другої «газової» війни. У результаті таких дій Росії від'ємне сальдо платіжного балансу України за роки правління Віктора Януковича склало 44 млрд. дол. США.

Олександр Власюк навів приклади створення Росією енергетичних проблем для тиску на Грузію та Литву у 2006 році, на Туркменістан у квітні 2009 року, та зауважив, що у 2014 – 2015 роках Росія перейшла до захоплення українських енергетичних активів у Криму та їх знищення на Донбасі. Він підкреслив, що зважаючи на такі дії, для України актуалізується завдання формування системи захисту критичної, зокрема енергетичної інфраструктури, яке має враховувати ті обставини, що суб'єктом зловмисних дій проти критичної інфраструктури може виступити держава-агресор, і що власниками більшості об'єктів критичної інфраструктури є приватні компанії. Зважаючи на це, відповідальність за захист критичної інфраструктури мають нести як відповідні державні органи, так і приватний сектор.

Представник Департаменту з політичних питань і політики безпеки Штаб-квартири НАТО в Брюсселі **Флоріан Енке** привітав учасників конференції та нагадав, що пройшло вже два роки, як Росія незаконно анексувала Крим, і в цьому брали участь регулярні російські війська, сили спецоперацій (так звані «зелені чоловічки»). Він згадав також масивну російську пропагандистську компанію з дискредитації нового Уряду України та зауважив, що всі ці дії Росії, як елементи гібридної війни, становили значне порушення міжнародного законодавства.

Флоріан Енке охарактеризував основні елементи гібридної війни та зробив висновок про необхідність врахування НАТО цієї нової реальності, у питаннях захисту критичної інфраструктури, зокрема й енергетичної, підвищення її стійкості. Він зауважив, що Україна є партнером НАТО, і наголосив на важливості реформ, які проводяться керівництвом Української держави. Він подякував організаторам конференції за можливість проведення діалогу щодо проблематики гібридної війни.

Президент Центру глобалістики «Стратегія XXI» **Михайло Гончар** привітав присутніх та стисло презентував матеріали дослідження Центру «Гібресія Путіна. Невоєнні аспекти війн нового покоління», які були надані учасникам конференції. Він підкреслив, що з новими викликами країни-члени Альянсу стикаються саме через призму дій Росії проти України, та висловив сподівання, що конференція відіграє роль «мозкового штурму» для того, щоб глибше зрозуміти сутність війн нового покоління, одним із різновидів яких є гібридна війна.

Директор Центру передового досвіду НАТО з питань енергетичної безпеки полковник **Гінтарас Багдонас** (м. Вільнюс, Литва) привітав присутніх та процитував слова стратега, філософа Карла фон Клаузевіца, що війна є продовженням політики іншими засобами. І, на його думку, ця формула є прийнятною для будь-якої, у т.ч. гібридної, війни. Він нагадав про використання енергоресурсів як інструменту проти України й інших країн. Розмірковуючи, як ми маємо протистояти цим викликам, доповідач висловив думку, що військові не

можуть самостійно виробити адекватну відповідь таким діям противника, проте рішення є, і воно просте – працювати разом, планувати, тренуватися та вчитися на конкретних ситуаціях. Гінтарас Багдонас зауважив, що Центр передового досвіду НАТО з питань енергетичної безпеки готовий до такої співпраці, може ділитися досвідом.

Першу дискусійну панель «Енергетика та гібридні технології ведення війн нового покоління» відкрив її модератор – **Олександр Суходоля**, завідувач відділу енергетичної та техногенної безпеки НІСД. Він нагадав присутнім доповідь Начальника Генштабу ЗС РФ Валерія Герасимова на загальних зборах Академії військових наук Російської Федерації у січні 2013 року, де той відобразив власне розуміння принципів гібридної війни, зростання ролі невійськових методів тиску на противника та інформаційного протиборства. Олександр Суходоля згадав аналітичну записку Джорджа Кеннана, в якій була сформульована концепція стримування Радянського Союзу часів Холодної війни, китайську концепцію «війни без кордонів», нові виклики, зокрема кіберзагрози та використання робототехніки. Він зазначив, що новим викликом у безпековій політиці є проблема використання енергетики у якості інструменту ведення війн нового покоління на та запропонував детальніше зупинитись на цьому питанні під час сесії.

З доповіддю «Нові інтерпретації гібридної війни у дослідженнях західних експертів. Погляд з України» виступив професор кафедри глобалістики, євроінтеграції та управління національною безпекою Національної академії державного управління при Президентові України **Володимир Мандрагеля**. Він зазначив, що на думку багатьох експертів, змістовні особливості гібридної війни були закладені у 1989 році американським експертом Вільямом Ліндом у теорії війн четвертого покоління. Володимир Мандрагеля згадав роботу співробітника ізраїльських спецслужб Йосі Купервасера «10 Lessons for Israel's Intelligence Reform», в якій автор зазначає, що зміна природи воєн стала одним із каталізаторів реформ ізраїльських спецслужб, і що на перший план виходить легітимність дій в очах громадян країни, міжнародної спільноти і навіть противника. Він також згадав роботи низки американських експертів, зокрема, аналітиків Франка Хоффмана та Расселла Гленна, в яких вони визначили гібридну загрозу як таку, де противник водночас застосовує адаптивну комбінацію звичайних, іррегулярних, терористичних та кримінальних методів діяльності, і це є комбінація дій як державних, так і не державних акторів. У своєму виступі Володимир Мандрагеля згадав і роботи низки інших експертів: російських вчених Сергія Чєкіна та Сергія Богданова, зокрема, їх публікацію «Природа і зміст воєн нового покоління», доповідь експертів Вашингтонського Центру аналізу європейської політики Лукаса і Мітчела, в якій зазначалося, що стаття 5 Вашингтонського договору не в змозі забезпечити надійний захист проти гібридної тактики Росії, а також роботи експертів Шведського Агентства оборонних досліджень Йохана Норберга та Фредріка Вестрелунда, статтю Марка Геліоті «Доктрина Герасимова та російська

нелінійна війна», які проаналізували січневу 2013 року доповідь Начальника Генштабу ЗС РФ Валерія Герасимова.

Володимир Мандрагеля навів узагальнюючі принципи гібридної війни, яких на його думку є сім, зокрема: (1) залежність та унікальність гібридних сил, їх структури, спроможностей від специфічного контексту конфлікту, (2) наявність специфічної ідеології всередині гібридних сил, які створюють внутрішню основу організації, (3) наявність екзистенціальної загрози потенційного противника, (4) гнучкий баланс між регулярними та нерегулярними силами, (5) динамічна комбінація військових і невійськових технологій, широке використання партизанських методів боротьби, які також можуть включати терористичні та кримінальні тактики, (6) перевага оборонних типів операцій, що не виключає окремі наступальні дії, (7) використання тактики змору, виснаження сил противника, як фізичних так і морально-психологічних. При цьому він навів відмінності гібридної війни від чисто партизанської: партизани не використовують важке озброєння (танки, артилерію тощо); партизани використовують тактику миттєвих атак і терористичних дій, уникаючи тривалих боїв; партизани іноді діють на територіях, які контролює противник, де нема ліній оборони; партизанські дії залежать від ставлення місцевого населення.

У своїй презентації Володимир Мандрагеля проаналізував також оборонні витрати країн світу, зокрема відмітив зростання протягом 2009 – 2014 років більш ніж у 2,5 рази витрат Росії, та зауважив, що в Стратегії національної безпеки США 2015 року найчастіше згадується економіка та енергетика. Володимир Мандрагеля також навів 8 (на його думку) фаз війн нового покоління, пояснив невоєнні методи ескалації конфліктів (з доктрини Герасимова) та згадав 4 фактори, що працюють на гібридну війну в колишніх республіках СРСР: (1) етнічна гетерогенність, зокрема в країнах Балтії; (2) наявність прихованих історичних кривд; (3) слабкість місцевих громадянських суспільств; (4) регіональна складність, яку Росія використовує краще, ніж інші зовнішні актори.

З доповіддю «Енергетика у воєнних конфліктах кінця XX – початку XXI століть. Західна оцінка» виступили експерти Центру передового досвіду НАТО з питань енергетичної безпеки **Ярослав Гаєк** та **Бенджамін Шорт**.

Ярослав Гаєк акцентував увагу на електричних мережах у гібридній війні, оскільки вся інша інфраструктура так чи інакше залежить від електричної. Він зауважив, що враховуючи велику протяжність ліній електропередач, забезпечити їх стійкість дуже складно. Також він зупинився на аналізі вразливості трансформаторних підстанцій та центрів управління, зокрема, останніх – до кібератак та ролі систем SCADA у забезпеченні стійкості електричних систем. Ярослав Гаєк навів приклади низки атак на електромережі, зокрема дій Ірландської Республіканської Армії у 1996 році; подій у 2013 році у каліфорнійській Кремнієвій долині, коли було

атаковано 17 трансформаторних підстанцій; подій у Пакистані у січні 2015 року, коли повстанці пошкодили декілька електроопор, що призвело до знеструмлення (блекауту) по всій країні. Він також розповів про проект щодо захисту критичної енергетичної інфраструктури, який наразі реалізується у Вільнюському Центрі передового досвіду НАТО з питань енергетичної безпеки та базується на аналізі подій в Україні, а також анонсував навчання щодо проблематики захисту критичної інфраструктури, яке має відбутися 17-20 травня 2016 року.

Бенджамін Шорт повідомив про інші роботи Центру, зокрема щодо досліджень місця енергетики в звичайних (конвенціональних) та гібридних конфліктах. Він навів приклад дослідження можливої ситуації з проривом дамби в іракському місті Мосул та розливу річки Тигр, від чого могло постраждати майже півмільйона людей, та наголосив на необхідності побудови ефективної системи захисту критичної інфраструктури.

З доповіддю «Енергетичний компонент у війнах нового покоління. Приклад російської агресії гібридного типу проти України» виступив президент Центру глобалістики «Стратегія XXI» Михайло Гончар. Він нагадав про роботу Центру «Гібресія Путіна. Невоєнні аспекти війн нового покоління» (гібресія – скорочено від гібридна агресія), та зауважив, що на думку фахівців Центру, авторами гібридної війни Росії проти України є Путін (головний ідеолог), Дугін («генеральний конструктор»), Сурков («головний технолог») та Герасимов (відповідає за воєнний компонент).

Михайло Гончар навів визначення гібридної війни, сформульоване Центром, як «комплексу різнорідних дій проти супротивника регульованої величини та комбінованого характеру, що застосовуються за певним алгоритмом, де воєнні засоби не є домінуючими», розповів про введене Центром поняття крипто-війни, яка передує гібридній війні і представляє приховану форму поступового, систематичного і довготривалого нанесення збитку супротивникові з метою максимального виснаження його потенціалу (у випадку України початком цієї фази можна вважати 2003 рік – рік прийняття Енергетичної стратегії Російської Федерації до 2020 року). Він зауважив, що одними із базових елементів такого типу війни було систематичне завищення ціни газу для України та інфраструктурні компоненти – створення маршрутів транспортування газу та нафти в обхід України.

Михайло Гончар підкреслив, що енергетична зброя є ефективною в умовах монополії зовнішніх поставок; профіциту трубопровідних потужностей; високих цін на енергоресурси; низьких температур взимку, коли зростаючий попит створює дефіцит палива. Водночас реалії 2014—2015 років (зниження цін, теплі зими, постачання газу в Україну за реверсом з Європи) зробили російський газовий важіль неефективним.

Переходячи до кримського етапу російської агресії, Михайло Гончар зазначив, що використання воєнного компоненту характеризувалося захопленням життєво важливої енергетичної інфраструктури. При цьому були захоплені не тільки кримські об'єкти, але й видобувні платформи на шельфі Чорного та Азовського морів. На його думку, таким чином був реалізований стратегічний задум Кремля: прибрати західних конкурентів російських держкомпаній, створивши невизначеність та неприйнятно високі військово-політичні ризики в зоні перспективного видобутку традиційних і нетрадиційних вуглеводнів на півдні та сході України.

Щодо російського проекту «Новоросія», Михайло Гончар навів основні рекомендації «Російської весни-2014» з ураження енергетичної інфраструктури: за сценарієм наступальних дій – артилерійські удари або удари БПЛА по вразливих об'єктах генерації; за сценарієм прихованих диверсійних дій передбачалося виведення з ладу системи подачі води на охолодження енергоблоків електростанцій; за кібер-сценарієм пропонувалися кібер-атаки проти ОЕС України. Він підкреслив, що хоча ці сценарії і не були реалізовані, проте у 2014 році були проведені диверсії на газопроводі Уренгой-Помари-Ужгород на Івано-Франківщині та Полтавщині, а окремі елементи кібер-сценарію були втілені 23 грудня 2015 року.

Щодо можливих дій Росії поза межами пострадянського простору, Михайло Гончар акцентував увагу на діях Росії, коли вона намагається активізувати чинники впливу на країни, через які проходять чи можуть пройти неросійські стратегічно важливі комунікації для постачання вуглеводнів до Європи. При цьому Росія розглядає такі проекти як конкурентні для російського Газпрому та діє на ураження таких магістралей. Як приклад він навів атаки на трубопроводи в східній Туреччині з боку робітничої партії Курдистану влітку 2015 року.

Наприкінці першої дискусійної панелі відбулося обговорення доповідей, доповідачі відповіли на низку запитань, зокрема щодо можливих шляхів повернення захопленої української видобувної інфраструктури на шельфі Чорного моря; необхідності забезпечення безпеки нових неросійських трубопровідних маршрутів постачання вуглеводнів до ЄС; співпраці Україна – НАТО; механізмів протидії російським «агентам впливу», зокрема, й в українському енергетичному секторі; необхідності протидії двом видам «зброї» гібридної війни – корупції (підкупу) та пропаганди (обману).

Другу дискусійну панель «Енергетика, енергетична політика, суб'єкти ринку» відкрив її модератор – директор Центру передового досвіду НАТО з питань енергетичної безпеки полковник Гінтарас Багдонас. Він нагадав присутнім, що в структурі НАТО є понад 20 центрів, які концентрують досвід та знання з різноманітних питань, та стисло розповів про завдання та роботу Вільнюського Центру передового досвіду НАТО з питань енергетичної безпеки. Гінтарас Багдонас повідомив учасників конференції про підготовлений

навчальний курс з питань енергетичної безпеки та навчання з питань захисту критичної інфраструктури, який має відбутися 17-20 травня 2016 року у Вільнюсі, а також повідомив про конференцію із захисту критичної інфраструктури в червні 2016 року у Варшаві.

З доповіддю «Безпека ЄС у сфері постачань газу. Уроки Північного потоку–2» виступила представниця Центру східних досліджень (Варшава, Польща) **Агата Лоскот-Страхота.**

Вона навела основні техніко-економічні характеристики проекту «Північний потік–2» та проаналізувала ключові ризики та наслідки для ЄС у разі реалізації цього проекту, зокрема проаналізувала позицію двох основних європейських груп акторів, одні з яких більше керуються комерційними чинниками та налаштовані розвивати співпрацю з Росією (у більшості вони представляють північ та захід Європи), а другі – політичними чинниками та налаштовані відносно Росії більш обережно, ставлячи розвиток співпраці з нею в залежність від подій в Україні (у більшості вони представляють Центральну та Східну Європу).

Агата Лоскот-Страхота навела також чинники, які, на її думку, наразі формують європейський газовий ринок, проаналізувала еволюцію розуміння в ЄС енергетичної безпеки з позиції газових постачань та зробила висновок, що наразі для Газпрому в Європі наступили часи невизначеності, зокрема з огляду на європейську політику диверсифікації постачань газу та зниження залежності від Росії. Водночас з її доповіді випливає, що наразі в ЄС більше питань щодо подальшого розвитку європейського газового ринку взагалі та проекту «Північний потік–2» зокрема, ніж відповідей.

З доповіддю «Енергетична безпека та енергетична політика України. Погляд НАТО» виступив представник Департаменту з політичних питань і політики безпеки Штаб-квартири НАТО в Брюсселі **Флоріан Енке.**

У першій частині доповіді Флоріан Енке охарактеризував роль НАТО у забезпеченні енергетичної безпеки країн-членів, виходячи з їх інтересів, та згадав саміти Альянсу в Ризі (2006 рік) та Бухаресті (2008 рік). Зокрема він підкреслив важливість спільних зусиль, співробітництва країн учасників та партнерів Альянсу, а також підтримки управління наслідками та захисту критичної енергетичної інфраструктури. Окремо було відзначено важливість Стратегічної Концепції НАТО, яка була обговорена на саміті в Лісабоні (2010 рік), де у порядок денний забезпечення енергетичної безпеки НАТО були включені питання підвищення готовності, сприяння захисту критичної інфраструктури та підвищення енергоефективності військ.

У другій частині доповіді доповідач порушив питання співробітництва Україна-НАТО. Зокрема, він виокремив важливість роботи Комісії Україна-НАТО та спільних заходів, які реалізуються в рамках щорічних національних програм та робочих груп. Флоріан Енке порушив також питання змін в Україні, зокрема у сфері забезпечення енергетичної безпеки, та міжнародної значущості забезпечення стабільності в Україні та безпеки транзиту газу її територією. Він зауважив, що реформи в енергетиці є найефективнішим заходом для підвищення стійкості до гібридних загроз. На його думку, створення конкурентних прозорих енергетичних ринків, демонополізація енергетичного сектору, диверсифікація джерел та маршрутів транспортування енергоресурсів, підвищення енергоефективності, сприяння власному видобутку має забезпечити просування України на шляху реформ.

З доповіддю «Енергетична безпека в Центральній та Східній Європі та діяльність російських державних компаній» виступив експерт з питань економіки та фінансів Празького інституту безпекових студій (Чехія) **Якуб Томашек**.

Доповідач сконцентрував увагу на діяльності двох російських державних компаній – Газпрому та Росатому, які посідають домінуючу позицію відповідно у постачаннях газу, ядерних технологій та ядерного палива до країн Центральної та Східної Європи.

Щодо ядерного сектору, то Томашек зазначив, що Росатом, на противагу можливим альтернативним постачальникам ядерних технологій, забезпечує левову частину фінансування будівництва АЕС, як це було реалізовано при будівництві Островецької АЕС в Білорусі та енергоблоків № 3 та 4 АЕС в Темеліні (Чехія). Характеризуючи газовий сектор, Якуб Томашек звернув увагу, що Газпром дотримується європейських правил, проте намагається максимально їх розширити для забезпечення своїх інтересів. Він також виокремив тяжіння Газпрому до монополізму та політизації постачань, їх непрозорості, нав'язування довгострокових контрактів на принципі «бери або плати», надання преференцій окремим споживачам. Водночас, на думку Томашека, Газпром намагається бути «звичайною» компанією, яка хоче отримувати прибуток, проте іронія полягає в тому, що головною загрозою для діяльності Газпрому в Європі є Кремль.

Наприкінці другої дискусійної панелі відбулося обговорення представлених доповідей. Доповідачі відповіли на низку запитань, зокрема щодо діяльності посередників на газовому ринку ЄС, що може нести в собі корупційну складову; можливості застосування статті 5 Північноатлантичного Договору у разі енергетичних проблем, у т.ч. пов'язаних з кібератаками на енергетичну інфраструктуру; необхідності забезпечення диверсифікації ядерного палива для європейських АЕС, зокрема АЕС Чехії; меж компетенції НАТО в питаннях енергетичної безпеки, зокрема на прикладі Північного потоку-2.

Третю дискусійну панель «Критична енергетична інфраструктура в умовах воєн нового покоління» відкрив її модератор – президент Центру глобалістики «Стратегія XXI» Михайло Гончар. Він запропонував детальніше зупинитися на практичних аспектах проблем захисту критичної енергетичної інфраструктури в умовах війн нового покоління та представив учасників третьої секції, зазначивши, що Національний інститут стратегічних досліджень вже кілька років займається згаданою тематикою та розробив Зелену книгу з питань захисту критичної інфраструктури.

З доповіддю «Енергетична інфраструктура: інструментальний вибір ведення війн нового покоління» виступив завідувач відділу енергетичної та техногенної безпеки НІСД Олександр Суходоля.

У своїй доповіді він порушив питання, наскільки енергетична інфраструктура є ціллю чи інструментом ведення війн нового покоління. Він нагадав вже згадане визначення гібридної війни, яке надав Франк Хоффман, та відзначив, що на прикладі України можна спостерігати, як саме держава-агресор виступає ініціатором зловмисних дій проти енергетичної інфраструктури, у т.ч. через використання кримінальних дій та актів тероризму.

Олександр Суходоля привернув увагу до окремих таких дій під протягом 2014 – 2015 років: захоплення об'єктів енергетики з метою їх подальшого використання; руйнування енергетичних об'єктів, систем енерго- та водопостачання; захоплення об'єктів з метою їх демонтажу та вивезення обладнання; перешкоджання відновленню пошкодженої інфраструктури та відновленню нормального життя громадян; кібератаки, які призвели до порушення енергопостачання окремих районів у кількох областях Західної України.

Доповідач також проаналізував наслідки подібних дій та виділив мотивації, які можуть стояти за ними, зокрема спричинення психологічного тиску як на населення, так і на уряд; спроба показати, що уряд не в змозі забезпечити нормальні умови життєдіяльності людей; завдання економічної шкоди як від захоплення, так і від руйнування об'єктів, а також перекладання відповідальності на Україну за відновлення інфраструктури; отримання тактичних переваг при проведенні військових операцій чи політичних переговорів; створення позитивного іміджу Росії та негативного України, у т.ч. шляхом розповсюдження фейкової інформації з питань енергопостачання. Загалом, на його думку, все це спрямоване на те, щоб створити хаос і невпевненість людей, що особливо небезпечно для тих країн, всередині яких є групи людей, які шукають привід, щоб виступити проти країни чи її уряду.
У доповіді Олександр Суходоля навів приклади заходів, які були реалізовані в Україні для захисту та відновлення критичної інфраструктури в умовах гібридної війни, зокрема, підкреслив важливість залучення міжнародних місій. Він також

поінформував про пропозиції НІСД стосовно шляхів подальшої розбудови в Україні системи захисту критичної інфраструктури, зокрема, реалізації положень Зеленої книги з питань захисту критичної інфраструктури.

З доповіддю «Проблеми забезпечення кібер-безпеки в контексті енергетичної безпеки» виступив співдиректор Інституту з проблем безпеки Бранденбурзького університету прикладних наук (Німеччина) **Гвідо Глушке**.

На початку презентації він стисло розповів про себе та про Інститут, навів посилання на низку книжок, присвячених кібербезпеці енергетичних, у т.ч. ядерних, об'єктів, згадав низку учбових курсів з цієї тематики які розроблено в Інституті з проблем безпеки. Гвідо Глушке навів спрощені схеми управління роботою АЕС та електричною системою (мережами), показавши як з часом змінювалися ці системи, зокрема, підвищувалася роль ІТ-технологій, та, відповідно, зростали кіберзагрози та ускладнювалися самі кібератаки.

Він підкреслив важливість використання методології розбудови системи захисту (зокрема, для ядерних об'єктів) на основі проектної загрози, яка на державному рівні описує основні характеристики правопорушників, та яка є основою для дальшої розбудови системи фізичного захисту ядерних об'єктів. Він також акцентував увагу на необхідності розмежування відповідальності операторів та держави, зростанні загрози військових атак, яка має розглядатися поза межами проектної загрози, а протидія якій є відповідальністю держави, та необхідності врахування кіберзагроз, у т.ч. тих, які виходять з боку ворожих держав.

У рамках аналізу кіберзагроз, Гвідо Глушке навів просту модель цілей, коли кібератака може бути чітко направлена проти якогось конкретного компонента системи чи обладнання, організації чи установки, випадкової цілі; відповідно до цих цілей можна охарактеризувати кібератаку – зрозуміти сутність загрози, визначити можливого нападника, спланувати превентивні дії чи дії у відповідь. При цьому він акцентував увагу на складності протидії чітко цілеспрямованій кібератаці, яка має унікальні характеристики, не має історичних аналогів, та якій не може протистояти жоден антивірусний захист. Переводячи це на «мову» проектної загрози, на думку доповідача, можлива максимальна кіберзагроза не тільки виходить за межі проектної, але може виходити навіть за межі спроможності держави, і для протистояння їй потрібно формувати культуру безпеки та розвивати міжнародну співпрацю.

З доповіддю «Захист критичної інфраструктури: новий вимір безпекової політики України» виступив завідувач сектору з питань захисту критичної інфраструктури та техногенної безпеки відділу енергетичної та техногенної безпеки НІСД **Дмитро Бірюков,** який представив особливості застосування положень Зеленої книги з питань захисту критичної інфраструктури.
Дмитро Бірюков поінформував присутніх про роботу, яка була виконана НІСД

у цьому напрямі протягом 4-х останніх років. Він зазначив, що у співпраці з Офісом зв'язку НАТО в Україні та Центром передового досвіду НАТО з питань енергетичної безпеки НІСД розробив Зелену книгу з питань захисту критичної інфраструктури в Україні. У цій книзі сформульовані стратегічні цілі та завдання державної політики у цій сфері, принципи побудови системи захисту критичної інфраструктури. Дмитро Бірюков також зауважив, що завдання створення такої системи визначені й чинною Стратегією національної безпеки України, та поінформував присутніх, що було зроблено у 2015 році.

Доповідач зазначив, що хоча до критичної інфраструктури НІСД відносить 10 секторів, проте, на його думку, саме енергетичний сектор є найбільш важливим. Він нагадав, що починаючи роботу над захистом критичної інфраструктури на основі існуючих норм було виділено 15 типів об'єктів, які мають бути захищені від певного типу загроз, оцінка ризиків робилася, виходячи з певного спектру можливих наслідків, а критерії віднесення теж були специфічні для кожної категорії об'єктів. При цьому не враховувалася взаємозалежність об'єктів та було відсутнє стратегічне бачення розбудови системи захисту критичної інфраструктури. Він представив своє бачення зв'язку системи захисту критичної інфраструктури з вже існуючими державними системами: боротьби з тероризмом, цивільного захисту, контррозвідувального захисту інтересів держави, кібербезпеки, фізичного захисту ядерних об'єктів та матеріалів.

Іншу частину своєї доповіді Дмитро Бірюков присвятив Директиві Єврокомісії 2008/114, яка стосується визначення загальноєвропейської критичної інфраструктури та тих кроків, які країни-члени ЄС мають робити для покращення захисту таких об'єктів. Поки що вона стосується енергетики та транспорту, але перелік секторів може бути розширений. Він акцентував увагу на двох головних «áкторах»: державах та операторах (власниках інфраструктури), та на тому, що для українських операторів це буде означати необхідність розробки планів безпеки, загальні вимоги до яких сформульовані у додатку до Директиви. Держава ж повинна визначити ті контактні точки (державні органи), які будуть взаємодіяти із загальноєвропейськими структурами. Доповідач також представив результати виконаного ним SWOT-аналізу впровадження цієї директиви в Україні, за підсумком якого зробив висновок на користь її впровадження.

Підсумовуючи свій виступ, Дмитро Бірюков висловив думку, що реальним кроком до створення системи захисту критичної інфраструктури має стати розгляд цього питання на засіданні Ради національної безпеки і оборони України.

Наприкінці третьої дискусійної панелі відбулося обговорення представлених доповідей. Зокрема, директор компанії «ТрансЕнергоКонсалтинг» Світлана Голікова зауважила, що багато у чому стійкість роботи Об'єднаної енергетичної системи України у 2015 році була обумовлена зменшенням споживання

електроенергії як всіма галузями економіки, так і населенням України. Вона зазначила, що для забезпечення стійкості роботи енергосистеми на перспективу важливим є розбудова українських енергетичних ринків на загальноєвропейських засадах, а також поставила питання щодо необхідності заміщення втрачених енергогенеруючих потужностей в Криму та на Донбасі з наданням переваги розподіленій, а не великій генерації.

Доповідачі відповіли на низку запитань учасників, зокрема: щодо можливості блекауту при низьких температурах взимку, який може бути наслідком кібератаки, замаскованої під розбаланс енергетичної системи; дискутували, чи розглядаються такі сценарії та що робиться для запобігання подібній ситуації.

Підводячи підсумки конференції Гінтарас Багдонас зауважив, що захід є гарним прикладом співробітництва та стимулом для його дальшого розвитку. Олександр Суходоля подякував всім учасникам за плідну роботу, представлені доповіді та підкреслив важливість співпраці як для України, так і для країн-членів НАТО та ЄС, що має підвищити стійкість країн до гібридних загроз.

Презентації учасників конференції доступні на сайті Національного інституту стратегічних досліджень
Доступ через лінк: http://www.niss.gov.ua/articles/2188/

Олександр Власюк,
Перший заступник директора НІСД
доктор економічних наук, професор,
член-кореспондент НАН України

Шановні колеги! Шановні зарубіжні гості!

Будь-яка війна тією чи іншою мірою є гібридною – тобто не обмежується лише збройним протистоянням, а складається з ідеологічних, пропагандистських, політичних, економічних, культурних, психологічних та інших елементів.

Водночас саме останніми роками, чітко вирізнилась тенденція зниження значущості військового чинника та поступового посилення з одного боку, економічної та пропагандистської складової ведення війн, а з іншого – парамілітарною, суміжною із військовою, складовою.

Останнє яскраво проявилося в діях російської сторони на Донбасі, коли агресор використовував бойовиків, місцевих «ополченців», кримінал та маргінес, на яких можна перекласти такі брудні речі, які держава, як сторона конфлікту, здійснювати не може, якщо слідувати міжнародному праву.

Триваюча в Україні гібридна війна, розв'язана російською стороною, проявила низку безпекових проблем. Сьогодні мова йде не про суперечку довкола визначення самого терміну «гібридності» (хоча спільне розуміння особливостей гібридної війни дуже важливе для успішного протистояння в такій війні). Мова йде про необхідність дальшого аналізу та усвідомлення сутності дій агресора, інструментів та засобів, які застосовує Росія.

Слід зазначити, що ця війна проявила нову сторону, це активне використання енергетики у якості інструменту нанесення поразки Українській державі.

Варто зазначити, що використання потенціалу енергетики як «енергетичної» зброї було відкрито проголошене у 2003 р. в Енергетичній стратегії Російської Федерації до 2020 р., де зазначалося, що потужний паливно-енергетичний комплекс Росії «є базою розвитку економіки, інструментом здійснення внутрішньої та зовнішньої політики». І це не просто декларація намірів, а реальний інструмент впливу, який неодноразово вже використовувався Росією у своїх інтересах.

Економічна складова російська енергетичної політики стала одним із інструментів підпорядкування України у передвоєнний період. У 2009 році за результатами другої «газової війни» Росія сформувала потужний інструмент тиску на Україну в енергетичній сфері, створила можливості для фінансового знекровлення її

економіки. У 2010-2013 роках стрімко зростало від'ємне сальдо платіжного балансу України (2010 р. – $3,0 млрд, $10,2 млрд, $14,3 млрд, $16,5 млрд, а загалом за роки правління В. Януковича – $44 мільярди).

Водночас, вплив на функціонування критичної інфраструктури інших країн як інструмент досягнення цілей у політичній та економічній сферах, так і зниження воєнно-економічного потенціалу держави в найкоротший термін також став широко використовуватись Росією.

Прикладом цього є майже синхронні підриви енергетичної інфраструктури, які припинили постачання природного газу та електроенергії до Грузії у січні 2006 р., що стало елементом подальшого тиску на Грузію. У 2006 р. на ремонт нафтопровід, який забезпечував постачання нафти на нафто- переробний завод у Мажейкяй у Литві, причому саме у момент, коли Литва вирішила продати завод польській компанії. Вибух на газопроводі у Туркменістані у квітні 2009 р. допоміг Росії призупинити дію незручного для неї договору із Туркменістаном і фактично усунути конкурента з європейського ринку.

З початком збройної агресії проти України Росія змінила акцент дій, з економічного виснаження економіки через укладання невигідних угод в напрямку фізичного захоплення енергетичних активів та їх знищення. При цьому енергетична інфраструктура стала предметом особливої уваги з боку агресора, оскільки її захоплення (чи руйнування) завдає не тільки значних економічних збитків, а й загрожує сталому функціонуванню системи життєзабезпечення суспільства загалом.

Росією, внаслідок анексії Криму, було захоплено не просто територію та об'єкти енергетики України, а через захоплення енергетичної інфраструктури (трубопроводів та компресорних станцій) фактично викрадено нафтовидобувні поля на шельфі та безпосередньо природний газ в обсязі 2 млрд м. куб. щорічно.

У подальшому, в окремих районах Луганської та Донецької областей, цілеспрямованими діями було фактично зруйновано значну кількість вуглевидобувних підприємств, здійснювалося блокування та руйнування транспортної інфраструктури. Своєю чергою це призвело до проблем із постачанням уже видобутого вугілля споживачам, передусім – на теплові електростанції, що стало викликом для стабільності функціонування всієї об'єднаної енергетичної системи України. Як наслідок – погіршилась і соціально-економічна ситуація не тільки у східних областях, а й загалом в Україні. Крім того, це сформувало довгостроковий виклик енергетичній безпеці держави загалом.

Далі було використано інформаційний складник «гібридної війни»: прийняті українським урядом антикризові рішення в енергетичній сфері були активно

використані для формування негативного ставлення до органів державної влади, посадових осіб та керівництва держави. Зазначена інформація активно використовувалась і для формування негативного іміджу України серед країн-сусідів та партнерів України.

Таким чином, порушення спроможності інфраструктури життєзабезпечення виконувати свої функції, стає інструментом гібридної війни, спрямованими на здійснення політичного тиску на уряд країни та психологічного впливу на населення, нанесення економічної шкоди країні.

При цьому, як свідчать події в Україні, суб'єктом зловмисних дій проти критичної інфраструктури може бути держава-агресор, а не лише окремі групи зловмисників (терористичні групи), як це вважалося до цього часу. У даній ситуації з огляду на те, що нині більшість суб'єктів господарювання в енергетичному секторі є приватними, відповідальність за забезпечення захисту критичної інфраструктури країни мають нести як відповідні органи державної влади, так і приватний сектор (оператори енергетичної інфраструктури). Інші зацікавлені суб'єкти, зокрема місцеві органи влади та населення, також мають залучатися до діяльності у цій сфері.

Саме тому завдання безпекової політики на сучасному етапі – дати ефективну відповідь на нові виклики, які постають в контексті виникнення війн нового покоління. Серед пріоритетних задач є формування в Україні системи захисту критичної інфраструктури, зокрема, енергетичної.

Сьогодні ми обговоримо основні загрози енергетичній безпеці України, з врахуванням викликів які породжують війни нового покоління та обговоримо основні задачі щодо формування системи захисту критичної енергетичної інфраструктури.

Гінтарас Багдонас
Директор Центру передового досвіду НАТО з питань енергетичної безпеки

Метою даної конференції є сприяння та підвищення ефективності створення надійних стійких і життєздатних інститутів та інфраструктури наших країн. Ми повинні знати суб'єктів, що є на нашому боці і їх сфери компетенцій. Що ці суб'єкти можуть зробити? Знаючи їх потенціал, ми створюватимемо синергію, спільну платформу знань і досвіду. Потрібно зробити все можливе, щоб працювати разом: планування і підготовка, особливо, спільна підготовка.

Місія Центру передового досвіду НАТО з питань енергетичної безпеки полягає в тому, щоб допомогти органам НАТО, країнам і партнерам та іншим цивільним і військовим органам шляхом надання експертних знань з усіх аспектів енергетичної безпеки. Литва та інші вісім країн вносять свій вклад в Центр, як забезпеченням кадрів, так і спільно використовуючи бюджет. В роботі Центру, в якості сприяючої країни-партнера, бере участь і Грузія. Сподіваюсь, що і Україна також приєднається до нашого Центру в один прекрасний день.

Прагнучи стати хабом (центром) визнаних знань і досвіду в області енергетичної безпеки для НАТО, її народів і країн-партнерів, Центр передового досвіду НАТО з питань енергетичної безпеки реалізує проекти в сферах безпеки, з дотриманням трьох аспектів енергетичної безпеки у відповідності до Уельського Саміту НАТО: 1) підвищення рівня інформованості з питань розвитку енергетики з наслідками для безпеки, 2) підтримка захисту критично важливої енергетичної інфраструктури та 3) підвищення ефективності використання енергії в збройних силах. Ці компетенції забезпечуються за рахунок трьох підрозділів Центру: 1) стратегічного аналізу і досліджень, 2) освіти, підготовки і навчання, 3) доктрини та концепції розвитку.

Основні заходи, які Центр передового досвіду НАТО з питань енергетичної безпеки планує реалізувати цього року:

- Командо-штабні навчання щодо захисту критичної енергетичної інфраструктури 17-20 травня 2016 року у Вільнюсі. Україна запрошується взяти участь у складі одного чи двох експертів.
- Курси з питань енергетичної безпеки у Вільнюсі в червні 2016 року і в Грузії в квітні 2016 року.
- Курс стратегічної усвідомленості енергетичної безпеки в школі НАТО в Німеччині у вересні 2016 року. Українські учасники запрошуються на цей курс.

Основні тези:

- *«Війна – це продовження політики іншими засобами»* – Карл фон Клаузевіц. Ця формула війни підходить для всіх поколінь війни. Природа війни не змінюється, змінюються механізми. Війна намагається зламати волю нації, застосовуючи різні засоби.
- Переходячи до сучасної війни нового покоління – існує багато прикладів такого роду нових війн: кібер-атаки, психологічні війни, пропаганда і маніпуляції, руйнування інфраструктури, саботаж, і т.п.;
- Як реагувати на такого роду виклики? Війна – це справа військових. Чи може військовослужбовець відповідно реагувати згідно плану дій по відношенню до невійськового типу агресії? Як протистояти, захистити інфраструктуру наших країн і підвищити стійкість? Яким є рішення?
- Відповідь проста – ми повинні працювати разом, щоб створити так званий «золотий трикутник»: залучення військових і урядових кіл в одному куті (з військовим та організаційно-планувальним досвідом і знаннями), наукового співтовариства з інтелектуальними здібностями – в іншому куті, і фахівців промислової сфери (або громадський сектор) – в третьому куті.
- Центр передового досвіду НАТО з питань енергетичної безпеки має навички та практчний досвід: ми розробляємо плани та готуємо людей, зокрема проводимо командо-штабні навчання щодо захисту критичної енергетичної інфраструктури. Цього року навчання присвячені тематиці захисту об'єктів електрогенерації та систем передачі енергії за участю мінімально 8 країн, що представляють всі сфери «золотого трикутника». Україна запрошується взяти участь у цих навчаннях.
- Центр передового досвіду НАТО з питань енергетичної безпеки готовий за запитом надати допомогу українським установам в тих сферах, що знаходяться в рамках нашої місії та діяльності.

Володимир Мандрагеля,
д.філос.н., професор, професор кафедри глобалістики,
євроінтеграції та управління національною безпекою
Національної академії державного управління
при Президентові України

Нові інтерпретації гібридної війни у дослідженнях західних експертів. Погляд з України

Поняття «гібридна війна» сьогодні доволі часто використовується у повсякденному вжитку, медіадискурсі, наукових дискусіях, проте поки його майже неможливо знайти у міжнародних документах, стратегіях безпеки країн ЄС та США. Разом з цим, на думку багатьох експертів, її змістовно-концептуальні особливості були вперше розвинуті американцем Вільямом Ліндом у теорії воєн четвертого покоління.

Її методологічну основу склала діалектика якості, де системоутворюючу роль виконує суперечність між тезою та антитезою (ідеєю та технологією). Війни попереднього, третього покоління (з 1918 р. до сьогодення), як вважає В. Лінд, більше ґрунтувалися на нових ідеях, ніж на нових технологіях. Тактика просочування, яку винайшли німці під час Першої світової війни, маневр військами та вогнем тощо стали домінуючими. Якщо до цього додати розвиток танків, авіації та іншої техніки, то цілком закономірною виглядає поява такої стратегії збройної боротьби, як кампанії "бліцкригів", орієнтованих скоріше на час, ніж на місце. Мала місце не тільки зміна тактики, яка зачепила воєнну культуру у цілому. Фокус уваги зосередився на противнику і результатах, які вимагали розвитку відповідальності за самостійні дії, а не тільки опанування стандартних методів досягнення цілей. За цих умов ініціатива стає більш важливою ніж слухняність. Динамічна зміна ситуації а не рутинні процедури стають пріоритетними. Керівництво стає терплячим до помилок, оскільки вони є невід'ємним наслідком ініціативи. На перший план виходить самодисципліна, а не зовнішній примус.

Війни четвертого покоління, на відміну від попередніх, ще більше базуватимуться на нових ідеях і матимуть незахідне «коріння». Тероризм, який не зачіпає традиційної військової сили і прямо уражає цивільне населення, вважається головним компонентом майбутніх «збройних змагань». При цьому підкреслюється, що, незважаючи на використання високоточної зброї, роботів, інформаційних технологій тощо, транснаціональна та недержавна основи тероризму у подальшому лише ускладнюватимуть боротьбу з ним. У війнах четвертого покоління держава втрачає монополію на насильство, оскільки з'являються впливові недержавні опоненти на кшталт аль-Каїди, Хамасу, Хезболли. В них, на думку В. Лінда, світ повертається до боротьби культур, а не

тільки держав. Ключовою причиною їхнього початку вчений вважає універсальну кризу легітимності держав, що створює умови для внутрішніх конфліктів і громадянських воєн.

Саме на теорію воєн четвертого покоління посилається заключний документ міжпарламентської конференції щодо Спільної зовнішньої політики і політики безпеки а також Спільної політики безпеки і оборони 4-6 березня 2015 р. (м. Рига). У п. 39 записано, що нові виклики безпеки, пов'язані з війнами 4-го покоління – гібридною війною, яка є комбінацією звичайних та незвичайних військових методів, елементів кібер-, економічної та інформаційної війни, а також політичного тиску.

А ось що пише високопосадовець ізраїльських спецслужб Йозеф Купервассер у своїй праці 2007 р. «10 уроків для реформи ізраїльської розвідки». Зміна природи воєн стало одним з головних каталізаторів реформи ізраїльських спецслужб. У минулому більшість воєн чітко визначалися часом, місцем, коли у противника був централізований процес прийняття рішень і очевидна військова присутність.

Однак, принаймні з 1982 р. все почало кардинально змінюватися. Протистояння стає майже безперервним, з короткотривалими високоінтенсивними діями. При цьому противник намагається діяти малими формуваннями, часто без пізнавальних знаків. Бойові дії почали вестися ширше у багатовимірному просторі з противником, який діє по всьому світі. Поняття захисту кордонів сходить нанівець, оскільки противник всюдисущий і складається з індивідів, які проходять через кордони або є громадянами тієї країни, де відбуваються дії.

Сьогоднішні «битви» є іспитом на витривалість й стійкість усього суспільства. Процес прийняття рішень опонентом носить прихований характер і складається з багатьох взаємопов'язаних елементів. Внаслідок цього відбулися зміни у індикаторах успіху. Замість території на перший план виходить легітимність в очах громадян країни, міжнародної спільноти і навіть противника.

Оскільки природа війни змінилася і легітимність набула першочергового значення, запроваджується нова тактика. Вона складається з власної інтерпретації подій і перекручувань або послаблень опису й коментарів противника, а також показ його реальних намірів.

Саме легітимність виступає основною причиною, за якою західні країни ведуть бойові дії відповідно до ліберальних норм і цінностей. Радикальні сили знають це і вибирають об'єктом нападу цивільне населення, яким у крайніх випадках прикривається як щитом [1, с. 7 – 9].

А вже у 2009 р. Франк Г. Хоффман та Рассел Гленн на конференції командування спільних сил США у лютому 2009 р. [2] визначили гібридну загрозу як таку, де противник водночас адаптивно застосовує складну комбінацію звичайних, іррегулярних, терористичних та кримінальних методів діяльності в оперативному просторі. Гібридна загроза вбирає в себе комбінацію державних та недержавних акторів.

Зауважу, що у 2009 р. з метою прогнозування спрямованості воєнних конфліктів майбутнього у НАТО був представлений документ «Multiple futures project – Navigating towards 2030» («Проект визначення множини варіантів майбутнього – навігація у 2030 рік») [3], у якому були представлені теоретичні прогнози щодо характеру можливих воєнних конфліктів та напрямки організації колективної безпеки. Зокрема, одним з напрямів розвитку Альянсу було визначено – пристосування до вимог гібридних загроз. Сутність такого типу загроз полягає в тому, що можливий противник уникатиме прямого зіткнення із силами НАТО в «конвенційних операціях», натомість застосовуватиме іррегулярні сили й асиметричні форми протиборства. Прогнозується, що поняття «гібридний противник» охоплюватиме регулярні й іррегулярні сили, терористичні та кримінальні елементи, котрі взаємодіятимуть між собою у різних «змішаних режимах». Слід зауважити, що «гібридний супротивник» не дотримуватиметься міжнародного права війни: цивільні особи використовуватимуться як постійно діючий «живий щит», який роз'єднує протидіючі сторони воєнного конфлікту.

Підполковник корпусу морської піхоти США Білл Немет у своїй докторській дисертації узагальнив досвід обох чеченських війн і характеризує гібридну війну, як: сучасну форму партизанської війни,... що використовує сучасні технології і оманні методи мобілізації. Б. Немет зазначає, що тактика чеченців часто знаходилась на межі між партизанською війною і тероризмом [4].

Вільямсон Мурей та Пітер Менсур визначають гібридну війну як конфлікт, до якого залучені звичайні збройні сили та іррегулярні формування (партизанські, повстанські, терористичні), які включають як державних так і недержавних акторів, які діють з метою досягнення спільної політичної мети. [5, с. 3]

Однак війна яку веде Росія в Україні, показує недосконалість таких визначень. Зокрема підкреслення поєднання звичайних та іррегулярних сил з одного боку занадто широке а з іншого – вузьке. Широке, оскільки значна кількість воєн в історії людства були таким поєднанням. У Другу світову війну активно застосовувалися рух супротиву, пропаганда, саботаж тощо.

В той же час при окупації Криму взагалі не було звичайної збройної боротьби. Деякі автори взагалі вважають гібридну війну скоріше як стратегію, ніж нову форму ведення бойових дій. Це стратегія, оскільки вона інтегрує використання

різноманітних інструментів національної могутності для досягнення зовнішньополітичних цілей з урахуванням цілей і спроможностей противника. Вона може охоплювати цілий ряд прийомів, поки вони керуються загальною метою.

Слід також звернути увагу на дослідження російських вчених С. Чернікова та С. Богданова, які протягом тривалого часу досліджують асиметричні дії [6] та війни нового покоління [7].

На анексію Криму першим (наприкінці березня 2014 р.) відреагував Центр аналізу європейської політики у Вашингтоні Center for European Policy Analysis (CEPA), де визначалася вразливість країн Центральної та Східної Європи. Автори (Е. Лукаш, В. Мітчелл) вважали, що Росія має військові спроможності та політичну волю для швидких та у цільовому відношенні обмежених дій. У доповіді зазначалося, що ст. 5. Вашингтонського Договору не в змозі забезпечити надійний захист проти тактики Росії, яку вона використовувала у Криму [8].

Експерти з шведського агенства оборонних досліджень Swedish Defence Research Agency (Totalförsvarets forskningsinstitut, FOI), Йохан Норберг та Фредерік Вестерлунд також аналізували стратегічні вибори Росії після Криму та доктрину Валерія Василоьвича Герасимова [9].

В статті «Доктрина Герасімова та російська нелінійна війна» Марка Галеотті є посилання на те, що НГШ має розробляти новий тип ведення війни після того як її почав Захід в арабській весні. Після неї він міг говорити як Росії повалить і зруйнує держави без прямої військової інтервенції [10]. Автор також помітив зауваження В. Герасімова щодо необхідності координації зусиль усіх державних установ, а також військової, розвідувальної та інформаційної операцій.

Деякі автори вважають, що у гібридній війні мало нового. Зокрема, естонка Мерле Майгре говорить, що комбінація атакуючих груп без пізнавальних знаків, місцевих агентів та загроза зовнішньої агресії використовувалася СРСР ще у 1924 р. [11].

Н. Попеску підкреслює, що реальною новелою російської операції в Україні була «близька до ідеальної» координація між різними силами та інструментами (дипломатичні, економічні, військові, інформаційні з однією добре організованої командної структури. А Оскар Джонссон та Роберт Сілі погоджуються з аналітиками FOI щодо високої ефективності координації зусиль. Плюс до цього почали писати росіяни. Зокрема книга Сергія Глазьєва «Украинская катастрофа. От американской агрессии к мировой войне?», яка вийшла у 2015 р. в Москві у видавництві «Книжный мир».

Інша книга військових експертів Руслана Пухова та Колбі Ховарда називалася Brothers Armed: Military Aspects of the Crisis in Ukraine, що розрахована на англомовну аудиторію. Тут представлений упереджений компаративний аналіз російських та українських ЗС, а також офіційна версія Кремля щодо легітимності захоплення Криму [12].

Слід також вказати на доповідь португальця Хуліо Міранди Калха на засіданні оборонного і безпековому комітету НАТО у серпні 2015 р., а також безліч статей, зокрема одна з останніх – Олександра Ланожка – «Російська гібридна війна та розширене стримування в східній частині Європи» в першому номері журналу International Affairs за 2016 р. [13].

В країнах Балтії тривоги посилилися після заяв Кремля у червні 2015 р. щодо можливості переглянути легітимність незалежності цих держав, яку вони отримали протягом 1990-1991 рр.

Естонія, Латвія та Литва мають у складі ЗС відповідно 2,800, 1,250 та 7,350 військовослужбовців, в той час як Росія на цьому напрямку утримує 250,000, вже не кажучи про повітряну, морську та ядерну підтримку.

Після розпаду СРСР в Естонії і Латвії було до чверті росіян і серед тих, хто не мав громадянства росіяни також складали більшість (7 та 12% відповідно). Це призводило до позбавлення політичних прав та безробіття.

Східноєвропейські держави вже мають переваги, оскільки вони члени НАТО і можуть закликати партнерів до консультацій, як це зробили Польща та Литва у квітні 2014 р., посилаючись на Ст. 4 Вашингтонського договору.

Експерти кажуть про розвинуту інфраструктуру НАТО в Європі. Але Росія буде уникати прямої військової конфронтації. Подивимося на різні аргументи, зокрема, М. Кроніга [14]. Військова присутність США та НАТО в країнах Балтії обмежена, війська США та тактична ядерна зброя переважно знаходяться в Західній Європі і це значно послаблює сили Альянсу. Його пропозиції: поширити військову присутність на країни Балтії, маючи передове сили в Східній Європі, незважаючи на заборони проти цього зазначені в Основоположному акті Росія – НАТО; допомогти країнам ЦСЄ з модернізацією та стандартизацією ЗС; розвивати і розміщувати в Європі нове покоління стратегічної ядерної зброї. Він також пропонує зміцнювати Східноєвропейські держави через військову допомогу, удосконалення розвідки та системи раннього попередження, кібербезпеку ВПС, тренінг, контроль кордонів та контррозвідку тощо.

На саміті в Уельсі у вересні 2014 р. члени НАТО погодилися на Readiness Action Plan, де серед іншого чотириразове збільшення повітряного патрулювання,

започаткування спостережних польотів над країнами Балтії та посилення військово-морських сил NATO [15]. Було НАТО також анонсували вістря сили (Spearhead Force), створення бригади до 5 тисяч особового складу з найвищим ступенем готовності. Влітку 2015 р. США прийняли рішення про розміщення у східній Європі важкого озброєння. Частішими стали тренування НАТО, включаючи Trident Juncture (восени 2015 р.), наймасштабніші за останні 13 років.

Проте готовність протистояти агресії на вищих рівнях не дорівнює цій спроможності на нижчих. Такий парадокс стабільності / нестабільності ще у 1960-х рр. описував Глен Снайдер.

Відтак посилення спроможності Альянсу на вищих рівнях надає гібридній війні більшої привабливості. При цьому агресор буде заперечувати свою участь. І навіть говорити про те, що існуюча криза інспірована ззовні невідомими силами. Відтак, попереду нас значною мірою чекають неочікувані події.

Література:

1. Kuperwasser Y. Lessons from Israel's Intelligence Reforms / Yosef Kuperwasser – The Saban Center for Middle East Policy at the Brookings Institute, 2007. – ANALYSIS PAPER, № 14. – 40 pp.
2. [Glenn R. W. «Thoughts on Hybrid Conflict / Russell W. Glenn // Small Wars Journal – [Електронний ресурс] – Режим доступу – http://smallwarsjournal.com/blog/journal/docs-temp/188-glenn.pdf?q=mag/docs-temp/188-glenn.pdf
3. Multiple futures project – Navigating towards 2030. Fleming [Електронний ресурс]. – Режим доступу: http://www.iris-france.org/docs/pdf/up_docs_bdd/20090511-112315.pdf
4. Hoffman F. G. Hybrid warfare and challenges / Frank G. Hoffman // Joint Force Quarterly – 1st Quarter 2009. – P. 34–48.
5. Williamson M. and Mansoor P. Hybrid warfare: fighting complex opponents from the ancient world to the present. / Murray Williamson and Peter R. Mansoor. – Cambridge: Cambridge University Press, 2012. – 321 pp.
6. Чекинов С.Г., Богданов С.А. Ассиметричные действия по обеспечению военной безопасности России / С.Г. Чекинов, С.А. Богданов // Военная мыслью – 2010. – № 3. – С. 13–22.
7. Чекинов С.Г., Богданов С.А. Природа и содержание войн нового поколения / С.Г. Чекинов, С.А. Богданов // Военная мыслью – 2013. – № 4. – С. 9 – 21.
8. Lucas E., Mitchell W. Central European Security After Crimea: The Case for Strengthening NATO's Eastern Defenses / E. Lucas – W. A. Mitchell // CEPA Report, No. 35, Center for European Policy Analysis – 25 March 2014, Washington D.C. – [Електронний ресурс] – Режим доступу – http://cepa.org/sites/default/files/The%20Case%20for%20Strengthening%20NAtos%20Eastern%20Defenses-%20%282%29.pdf

9. Norberg J., Westerlund F. Russia and Ukraine: Military-strategic options, and possible risks, for Moscow / J. Norberg, F. Westerlund // RUFS Briefing, No. 22, FoI, April 2014, Stockholm. – [Електронний ресурс] – Режим доступу – http://www.foi. se/Global/V%C3%A5r%20kunskap/S%C3%A4kerhetspolitiska%20studier/Ryssland/ Briefings/ruFS%20Briefing%20No.22.pdf
10. Galeotti M. 'The 'Gerasimov doctrine' and Russian Non-Linear War / M. Galeotti // In Moscow's shadows – 6 July 2014. – [Електронний ресурс] – Режим доступу – https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/
11. Maigre M. Nothing New in Hybrid Warfare: The Estonian Experience and Recommendation for NATO / M. Maigre // Policy Brief, February 2015, The German Marshall Fund of the United States, http://www.gmfus.org/publications/nothing-new-hybrid-warfare-estonian-experience-and-recommendations-nato.
12. Pukhov R., Colby H. (eds.), Brothers Armed: Military Aspects of the Crisis in Ukraine. East View Press, Minneapolis, 2014. – 228 pp.
13. Lanoszka A. Russian hybrid warfare a and extended deterrence in eastern Europe / Alexander Lanoszka // International Affairs – 2016. – Vol. 92. – No 1. – P. 175 – 195.
14. Kroenig M. Facing reality: getting NATO ready for a new Cold War. / Matthew Kroenig // Survival. – 2015. – No 57 (1). – P. 49–70.
15. NATO's Readiness Action Plan, fact sheet, Dec. 2014. – [Електронний ресурс] – Режим доступу–http://www.nato.int/nato_static_fl2014/assets/ pdf/pdf_2014_12/20141202_141202-facstsheet-rap-en.pdf, accessed 13 Nov. 2015.

Михайло Гончар
Президент Центру глобалістики «Стратегія XXI»,
консультант Секретаря РНБО України 1996-2000 р.р.

Енергетичний компонент в війнах нового покоління. На прикладі агресії РФ проти України

Шановні пані і панове,

Передусім хотів би висловити вдячність за спільні зусилля Центру передового досвіду НАТО з питань енергетичної безпеки, Національного інституту стратегічних досліджень, що були підтримані Міжнародним фондом «Відродження» та Київським міжнародним енергетичним Q-клубом щодо організації цієї конференції.

10 років тому у лютому 2006 року Емма Сімпсон з BBC написала статтю «**Russia wields the energy weapon**». Вона відзначила, що **енергоресурси наділяють Росію значною політичною силою і світ хоче побачити, як ця сила буде використовуватися**. Через 10 років ми можемо констатувати, що РФ доволі успішно використовує енергоресурси та інфраструктуру їх доставки для вирішення завдань геополітичного та геоекономічного характеру. Енергетичні мотиви також присутні при тих чи інших діях Росії, в тому числі і військових. Розглянемо це на прикладі російської агресії гібридного типу проти України. Скорочено ми називаємо її гібресією. Про її особливості йдеться у новій роботі Центру глобалістики «Стратегія XXI», яка представлена вам на цій конференції, і яка має назву « Гибрессия Путина. Невоенные аспекты войн нового поколения». Це частина нашої роботи в рамках проекту, підтриманого свого часу МФ «Відродження».

Агресія гібридного типу – це комплекс різнорідних впливів на супротивника регульованої величини і комбінованого характеру, що застосовуються по варіативному алгоритму, де військові засоби не є домінуючими, їх застосування ретельно маскується і заперечується, а сам акт агресії генерує невизначеність, що ускладнює його ідентифікацію.

Глибинною сутністю гібридної війни є багатовимірна цілеспрямована полідеструкція, тобто руйнування однією державою іншої комплексним комбінованим застосуванням сил і засобів військового і невійськового характеру в різних вимірах (політичному, економічному, військовому, гуманітарному та ін.), але направлено концентрованих на меті знищення противника не тільки і не стільки на полі бою, скільки шляхом підриву його життєвих потенціалів, насамперед, зсередини при певних синхронізованих діях ззовні.

Крипто-війна є окремом етапом агресивних дій в неявному вигляді, війна яка не сприймається як така, своєрідна недовійна. Вона є обов'язковим етапом, що передує подальшим, але не є фазою самої гібридної війни. **Крипто-війна – це прихована форма поступового, систематичного і довготривалого нанесення шкоди супротивникові з метою максимального виснаження його потенціалу до часу, коли буде прийнято рішення про агресію класичного або гібридного типу.**

Гібресія має певну послідовність дій і етапність. Ключові етапи тою чи іншою мірою характеризуються **енергетичними важелями, цілями та мотивами** у діях агресора. Умовно нульовий етап, що передує агресії – крипто-війна, в українському випадку характеризується довготривалим застосування газового важеля впливу.

У випадку України, базовим елементом крипто-війни став енергетичний, а точніше газовий. Використовуючи гіпертрофовану залежність економіки України від постачань газу з РФ та збільшуючи ціну газу, РФ здійснювала систематичне та послідовне фінансове виснаження економіки України. Паралельно нав'язувались непрозорі схеми газового бізнесу з корупційним підгрунтям, культивувалась корупція на вищих щаблях влади, у владу просувалась як явні та приховані лоббісти, так і креатури спецслужб.

Іншим елементом крипто-війни був інфраструктурний. Починаючи з 2000-х Росія реалізовувала курс на створення безтранзитних нафто- і газопровідних систем в обхід України. Були побудовані і введені в експлуатацію Балтійська трубопровідна система - 1 з терміналом в Приморську і Балтійська трубопровідна система - 2 з терміналом в Усть-Лузі для безтранзитного експорту нафти. Були реалізовані проекти газопроводів «Блакитний потік» через Чорне море і «Північний потік» через Балтику, що знизило транзитні доходи України. Постійно йшлося про необхідність створення консорціуму з управління ГТС України за участю «Газпрому», що означало б по суті встановлення контролю над основними промисловими активами країни через поставки газу.

Крипто-війна є важливою підготовчою фазою для подальшого розгортання агресії. Вона може тривати досить довго – роками, виснажуючи економіку противника. Україна переплачувала Газпрому за придбаний у великих обсягах газ і недоотримуючи доходи внаслідок скорочення транзиту через її територію. При цьому пропаґандистськи Росія все представляла таким чином, що вона поставляє Україні найдешевший газ, підтримуючи її економіку на плаву.

Оцінка енергетичної активності Росії виконувалася у Європі лише у системі бізнес-координат. Аналіз поведінки Росії в 2000-х роках показує, що вона послідовно йшла до використання енергоресурсів як енергетичної зброї, ретельно

маскуючи це під комерційні суперечки з покупцями російських вуглеводнів на пострадянському просторі. Енергетична зброя є ефективною в умовах монополії зовнішніх поставок, профіциту трубопровідних потужностей, високих цін на енергоресурси, низьких температур взимку, коли зростаючий попит створює дефіцит палива. **Зниження нафтових і, відповідно, газових цін, починаючи з літа 2014 року, вплив Ель-Ніньо на метеорологічні умови у Східній Європі (теплі зими 2014-2015 та 2015-2016 р.р.), реверсні поставки з ЄС зробили неефективним застосування Росією проти України газового важеля.**

2. Етап задіяння воєнного компоненту характеризується захопленням життєво важливої енергетичної інфраструктури. Кримська кампанія характерна тим, що були захоплені не тільки енергетичні об'єкти на півострові, але й видобувні та бурові платформи на шельфі Чорного і Азовського морів у 2014 році поза межами територіального моря. Тут в України стався найбільший прикрий збій із захистом цих видобувних і бурових платформ Вони виявилися захоплені російським десантом, який був висаджений на платформи не відразу, а майже через 3 тижні після початку дифузного вторгнення до Криму. Головною проблемою виявилося те, що в умовах управлінського хаосу Морська прикордонна служба не виконала Ст. 31 Закону України «Про виключну (морську) економічну зону України», де чітко зазначено *«Охорона суверенних прав України у виключній (морській) економічній зоні та контроль за реалізацією прав і виконанням зобов'язань інших держав, українських та іноземних юридичних і фізичних осіб, міжнародних організацій у ній здійснюється Державною прикордонною службою України».* Так само і ВМС України виявились не здатними до рішучих дій, оскільки були блоковані в бухтах Севастополя і Донузлава. Однак, дивізіон охорони водного району, який базується в Одесі міг виконати необхідні дії. Сили і засоби для захисту платформ також могли б бути доставлені за допомогою вертольотів армійської авіації, враховуючи, що основні платформи обладнані злітно-посадковими майданчиками. Однак, нічого цього не сталося. Управлінський хаос того періоду та бажання окремих осіб ускладнити розслідування оборудок з «вишками Бойка» - це те, що можливо колись буде з'ясовано в ході відповідних процесуальних дій.

Втрата 1,6 млрд. куб.м. шельфового газовидобутку із загального рівня в 21,5 млрд. куб.м. внутрішнього видобутку не є чутливою для України, оскільки цей газ надходив лише на півострів. Але тим не менше це означає втрату практично всієї інфраструктури морського газовидобутку, яка розвивалася в Україні з 80-х років. Також втрачена можливість розширення шельфового газовидобутку для чого було придбано 2 новітніх бурових платформи, які також були захоплені. За рахунок програми буріння передбачалося збільшити газовидобуток на шельфі до 8 млрд. куб. м в рік в 2020 році, що істотно дозволило б зменшити імпорт газу з Росії. До того ж з втратою шельфових родовищ, Україна втратила і масштабні проекти на глибокій воді, куди прийшли великі західні компанії.

З огляду на це та враховуючи традиційну схильність Росії до створення антиконкурентних та монопольних схем, одним з мотивів окупації Криму був енергетичний. Окупація півострова дає Росії вирішення низки питань стратегічного характеру:

- ліквідація перспективних проектів розвідки і видобутку газу в Чорному морі, які ініціювала Україна із залученням провідних європейських і американських компаній, що є викликом для російських державних компаній;

- витіснення з північного сектора Чорного моря провідних американських і європейських нафтогазових компаній, що є конкурентами російських державних компаній;

- позбавлення України доступу до основної частини шельфових родовищ газу і перспективних запасів вуглеводнів в Чорному морі;

- створення передумов для корекції маршруту трансчорноморського газопроводу (на той час «Південний потік», згодом – «Турецький», нещодавно – «Болгарський», поточно – без назви) з частковим прокладанням його поблизу або й через Кримський півострів і шельфову мілководну зону Чорного моря.

Можна констатувати, що три з чотирьох означений цілей досягнуто. Четверта – в роботі. Хоча вона й виглядає на сьогодні безперспективною з огляду на загальну непотрібність подібного проекту для ЄС, тим не менше робота у цьому напрямку продовжується й останнім часом вона активізована.

Ми спостерігаємо, що окупант – Росія – має серйозні проблеми з енергетичним забезпеченням півострова. Чому це має місце? Невже у Кремлі не знали про енергодефіцитність Криму, що становила ~83% по електроенергії, 100% - по вугіллю, 100% - по нафтопродуктах. Практично, Україна вивела Крим на 100% забезпечення по газу завдяки інвестиції НАК «Нафтогаз України» в розширення експлуатаційного буріння на мілководному шельфі Чорного моря у 2011-2013 р.р.

Відповідь на дане питання у тому, що насправді у Кремлі це чудово розуміли, але не вважали це чинником ризику, оскільки після Кримської кампанії мав стартувати проект «Новоросія». Реалізація цього проекту в його початковому вигляді – сепарація 8-10 областей сходу та півдня України мала автоматично вирішити усі питання енергетичного та ресурсного забезпечення Криму, зокрема, по електроенергії та воді. Понад те, енергодефіцитною виявилась би Україна, точніше те, що від неї лишилось би, оскільки основні джерела видобутку первинних енергоресурсів потрапили би на територію так званої «Новоросії» - майже весь вуглевидобуток, 4/5 видобутку природного газу, 9 з 15 енергоблоків АЕС, левова частка теплової енергетики. Проект «Новоросія» зазнав краху, тому Крим автоматично виявився в скрутному енергетичному та ресурсному становищі.

Міністерство енергетики Росії оперує цифрою потреб Криму в електроенергії в 1442 Мвт потужності. Водночас, якщо усі проекти перекидання потужностей в Крим по енергомосту та створення додаткової генерації на самому півострові будуть реалізовані, то сумарна потужність становитиме 2225 МВт, що в 1,8 рази більше, аніж традиційні до 2016 року постачання в Крим з материкової України. **Очевидно, що більша, аніж до окупації потужність пов'язана із зростаючими потребами угруповання російських збройних сил на території півострова, а також перспективних планів його нарощування. Побічно, це є підтвердженням масштабних планів розгортання додаткової воєнної інфраструктури, що потребуватиме значних обсягів енергоспоживання.**

3. Тепер розглянемо енергетичний компонент під час військової фази гібресії. За наявною інформацією, в Росії відпрацьовувалися варіанти критичної поразки енергетичної інфраструктури України ще з весни 2014 року, коли стартував «проект «Новоросія». Цілями впливу повинні були стати об'єкти об'єднаної енергосистеми України і газотранспортної системи. Передбачалося, що внаслідок ураження ключових об'єктів енергетичної інфраструктури, Україна стане енергодефіцитною, з колапсуючими ОЕС і ГТС. Тому, за логікою розробників сценарію, буде змушена звертатися до Росії за допомогою, щоб пройти зимовий період. Умовою Росії буде визнання «Новоросії» Києвом, підписання «мирного договору», виведення з «Новоросії» «окупаційних військ київської хунти».

У відповідних аналітичних матеріалах сепаратистів, зокрема, «Украина во тьме: практика», констатувалося, що «ахіллесовою п'ятою» генерації в ОЕС України є енергокомплекс в Енергодарі Запорізької області. Відзначалося, що *«до його складу входять, фактично лише рознесені парканом, Запорізька ГРЕС і Запорізька АЕС ... Обидві електростанції є найбільшими в Україні за встановленою потужністю, а АЕС ще й найбільшою електростанцією в Європі і колишньому СРСР»*. Ось приклад однієї з рекомендацій щодо дій в районі Енергодара: *«Особливої важливості набуває питання виведення з ладу обох запорізьких електростанцій, перш за все, атомної. Крім зазначалося раніше можливості зробити це атакою проти градирень АЕС, більш ймовірне досягнення успіху при одночасному відключенні ліній 750 кВ від підстанції «Дніпровська» в бік Лівобережжя. У разі успіху такої акції, частина обладнання АЕС буде неминуче відключена ... Якщо ж поєднати її з ударом по лінії 750 кВ, що відходить від цієї ж підстанції на захід, то вийде ... сценарій «блек-ауту» в Одеській і Миколаївській областях, здатний викликати аварійне відключення Південно-Української АЕС. Атака може початися з виведення з ладу магістральної лінії Західна Україна – Донбас в двох місцях на території Черкаської області. Цей захід ... порушить стійкість об'єднаної енергосистеми в цілому ... »*

В цілому ж пропонувалися й інші дії, а не тільки виведення з ладу міжсистемних ліній електропередач, зокрема: кібер-атака проти системи оперативного диспетчерського управління ОЕС України, а також вогневий удар по вразливих

місцях об'єктів генерації – градирні АЕС, димові труби ТЕС, система подачі води. Це в комплексі мало б привести до «системної аварії в масштабах всієї об'єднаної енергосистеми». Пропонувалися інструменти атаки – артилерія, або безпілотні літальні апарати. Але це за сценарієм відкритих наступальних дій. За сценарієм прихованих диверсійних дій передбачалося вивести з ладу систему подачі води на охолодження енергоблоків. Причому, пропагандистськи це повинно бути подано таким чином, що диверсія виконана «київської хунтою» з метою звинуватити «ополченців».

Як відомо, особливе значення і для України, і для ЄС має ГТС, через яку йде забезпечення газом як своїх, так і значної частини європейських споживачів. Значущим є високий рівень інтерконнектингу магістральних трубопроводів, що забезпечує безперебійність поставок газу в разі аварій або інших надзвичайних ситуацій. Це те, чого немає в інших маршрутах транспортування, іменованих «Газпромом» як альтернативні до українських газопроводів: Ямал – Європа, «Блакитний потік», «Північний потік». Аварія на будь-якому з цих напрямків автоматично призведе до припинення поставок газу. В Україні зовсім інакше. У 2007 році мали місце два серйозних технічних інциденту на магістральному газопроводі Уренгой – Помари – Ужгород. На ліквідацію наслідків аварій в обох випадках знадобилося більше 2 тижнів. Однак, газопостачання ЄС не припинялося ні на хвилину, замість аварійного газопроводу були задіяні інші. Через 7 років наша ГТС пройшла і продовжує проходити випробування «гарячим сценарієм» вже третій рік. Незважаючи на те, що в 2014 році в травні і червні мали місце диверсійні дії на тому ж газопроводі Уренгой – Помари – Ужгород, це не спричинило за собою переривання поставок газу в ЄС. Слід зазначити, що за нашими оцінками, для повного переривання поставок газу в ЄС з території України необхідно провести одночасний підрив в 29 місцях об'єктів ГТС, що є практично нездійсненним завданням в умовах гібридної війни.

4. Забезпечення України газом завжди залежало від поставок з Росії або через Росію. І газовий сектор традиційно був вразливим місцем для України в її відносинах з РФ. Але по вугіллю Україна була завжди незалежною, добуваючи достатню його кількість і навіть частково експортуючи. Найбільші ризики для України в зимовому сезоні 2015-2016 р.р. були пов'язані з електро- і теплової енергетикою. Дефіцит антрацитових марок вугілля, основний видобуток яких знаходиться на окупованих територіях Донбасу, міг спровокувати дефіцит виробництва електроенергії і тепла на температурному екстремумі. Однак цього не трапилось завдяки українським АЕС, які виробили 2015 року 55,5% усієї електроенергії.

Інша загроза, яка позначилась – це кібер-атаки на об'єкти ОЕС України. Можу відзначити, що за 10 днів до початку атак наш Центр попереджав про високу ймовірність такого сценарію, особливо на температурному екстремумі. Слід,

однак, відзначити, що стійкість ОЕС виявилась більшою, аніж уявлялось. Я не буду заглиблюватися у кібер-тематику. Лише зазначу, що за деякими експертними оцінками, підготовка до кібер-впливів на ОЕС України була розпочата 2013 року – ще до початку війни проти України. За висновками американських експертів, що , що стали доступні в рамках публікації матеріалу «Розслідування Wired: як відбувалася атака на «Прикарпаттяобленерго?»: ***«хакери, які атакували українські електростанції … ретельно планували напад протягом багатьох місяців. Спочатку вони провели розвідку внутрішніх мереж, потім добули дані операторів, а потім зробили синхронну атаку»***. Тому, кібер-загрози для критично важливої енергетичної інфраструктури в умовах гібридної агресії РФ проти України знаходяться на передових позиціях.

Висновки.

Газовий важіль впливу на Україну в ході гібресії виявився неефективним з огляду на впливи Ель-Ніньо (теплі зими), падіння цін на нафту та реверсні постачання газу з ЄС до України.

Враховуючи економічну несамодостатність окупованих територій як Криму так і окремих районів сходу України, зберігається мотив Росії сполучити ці території. При цьому існує як суто воєнний мотив, так і енергетичний резон.

Росія використовуватиме проксі-методи для протидії європейським спробам диверсифікувати постачання газу до ЄС та реалізувати проекти постачання газу з неросійських джерел.

Потрібний посилений моніторинг російської активності всередині країн-членів НАТО та ЄС. Росія, за логікою війни нового покоління, багато в чому буде діяти зсередини, а не ззовні, в тому числі використовуючи лоббістські та корупційні механізми, напрацьовані за останні десятиліття вуглеводневих постачань до Європи.

Росія буде діяти на кібер-ураження європейських енергетичних мереж, намагаючись спровокувати масштабний блек-аут.

Відповідно до технологій протидії агресіям гібридного типу, необхідна альтернативна модель примусу до миру невоєнним шляхом або ж створенням для нього сценарію мультикризи зсередини (розширення економічних санкцій ЄС на енергетичний сектор – поступове заміщення російської нафти та газу вуглеводнями з альтернативних джерел).

Це далеко не вичерпний перелік того, що можна робити заради примусу агресора до миру й відходу з окупованих територій України.

Дякую за увагу!

Флоріан Енке
Департамент з політичних питань і політики безпеки,
Штаб-квартира НАТО (Брюссель, Бельгія)

Енергетична безпека та енергетична політика України. Погляд НАТО.

В своїй доповіді я висвітлю три питання. По-перше розгляну роль НАТО в енергетичній сфері, по-друге коротко зупинюся на тому, як ми вирішуємо питання енергетичної безпеки в рамках Особливого Партнерства між НАТО та Україною та по-третє, висвітлю деякі аспекти стосовно енергетичної політики.

Роль НАТО в забезпеченні енергетичної безпеки

Дозвольте мені розпочати з обговорення того, яку саме роль відіграє НАТО в енергетичній безпеці, як ми підійшли до рішення цього питання, і на яких напрямках роботи зосереджуємо увагу.

Слід зазначити, що обставини та хід подій в Україні завжди були тим важливим фактором, який підвищував інтерес Альянсу до питань енергетичної безпеки. Все почалося з газової суперечки між Росією та Україною в 2006 році, яка протягом декількох днів залишила без газопостачання кілька країн в Центральній і Східній Європі. Це був той «тривожний сигнал», який порушив питання щодо впливу енергетичних ризиків на національну безпеку та суверенітет.

Ці події стали приводом дискусії про те, що місія НАТО по забезпеченню безпеки її членів повинна беззаперечно включати в себе енергетичну складову. Це не дивно, що країни Центральної та Східної Європи відносилися до найбільш активних прихильників такого плану, враховуючи, що вони відновили свій суверенітет в не дуже далекому минулому, а їх залежність від поставок російського газу була особливо високою.

Проте, визначення ролі НАТО в забезпеченні енергетичної безпеки не було легким завданням, і я можу сказати, що воно ще й досі незавершене. Насамперед, в значній мірі невійськовий характер енергетичних відносин зіграв певну роль. Страх Альянсу бути втягнутим в суперечку з Росією був ще одним з факторів, принаймні, для багатьох «старих» членів Альянсу.

У 2006 році Ризький саміт прийшов до висновку про те, що інтереси безпеки Альянсу можуть постраждати в результаті порушення постачання життєво важливих ресурсів. Союзники вирішили проводити консультації щодо найбільш нагальних ризиків у сфері енергетичної безпеки, з тим, щоб визначити ті сфери, в яких НАТО може підвищити потенціал. Альянс замовив звіт щодо ролі НАТО в забезпеченні енергетичної безпеки, який потім був підготовлений до проведення наступного саміту в Бухаресті в 2008 році.

У зв'язку із обмеженнями, які я згадував раніше, основні принципи та напрямки діяльності НАТО в сфері енергетичної безпеки, що були сформовані на саміті в Бухаресті були вельми стриманими. Насправді, вони обмежувалися лише обміном розвідувальною інформацією стосовно розвитку енергетики, політичними консультаціями, взаємодією із зацікавленими країнами-партнерами і обговоренням кращих практик щодо захисту критично важливої енергетичної інфраструктури в НАТО.

Для порівняння, нова стратегічна концепція НАТО, погоджена в Лісабоні в 2010 році, мала досить різкі формулювання, із зазначенням мети розвитку потенціалу для сприяння енергетичної безпеки, в тому числі захисту найважливіших об'єктів енергетичної інфраструктури та транзитних зон і маршрутів, а також співпраця з партнерами з числа союзників. Тим не менш, це стало реальним, практичним розвитком ситуації, ніж просто формулюванням, що зробило роль НАТО в забезпеченні енергетичної безпеки більш реалістичною. НАТО почало свою операцію по боротьбі з піратством біля берегів Сомалійського півострову, даючи Альянсу безпосередню роль в захисті поставок енергії. Причиною було збільшення частоти терористичних і кібер-атак на енергетичну інфраструктуру в усьому світі. Використання енергетики в рамках «гібридної» стратегії військових і невійськових загроз, що застосовується Росією в умовах кризи Україна-Росія з 2013 року стало ще одним явищем, яке Альянс не може ігнорувати.

Все це не робить НАТО енергетичною організацією. Але Альянс володіє деякими унікальними характеристиками, які дозволяють йому сприяти в розвитку енергетичної безпеки союзників і країн-партнерів, на основі свого членства і широкого спектру дій країн-партнерів, платформою для обміну розвідувальною інформацією і політичними консультаціями, яку пропонує НАТО, а також потужністю у військовому плануванні та управлінні. Таким чином, в кінцевому рахунку три елементи складають програму НАТО з енергетики:

- Підвищення розуміння стратегічних умов енергетичного розвитку та їх наслідки для безпеки, що означає, зокрема: політичні консультації (між союзниками і з країнами-партнерами), обмін розвідувальною інформацією та внутрішній аналіз того, як розвиток енергетики може вплинути на політику і операції НАТО.
- Підтримка захисту важливої енергетичної інфраструктури. В той час як це залишається національною відповідальністю, обмін передовим досвідом (наприклад, шляхом проведення семінарів і командно-штабних навчань) є найчастіше запропонованим пунктом співпраці НАТО, опираючись на енергетичну безпеку. Ще одним фактором є досвід НАТО в антикризовому управлінні та в управлінні наслідками, спільно з плануванням цивільної оборони.
- Покращення енергоефективності в армії, де НАТО розпочало об'єднувати національні зусилля.

Кілька країн-партнерів НАТО висловили свою зацікавленість у співпраці в

галузі енергетичної безпеки, але їх інтереси істотно розрізняються. Деякі з них в основному зацікавлені в захисті морської енергетичної інфраструктури та боротьбі з піратством, інші орієнтовані на підготовку та доступ до інформаційно-консультаційних послуг щодо захисту критично важливих об'єктів енергетичної інфраструктури. НАТО не тільки посилює регулярні контакти, але і прагне до розвитку налагодженої партнерської співпраці. Очікується, що енергетична безпека стане постійним елементом в підготовчих та навчальних програмах НАТО, щоб дати дипломатам і військовим лідерам більш глибоке розуміння питань енергетики, включно з конкуренцією за ресурси та зміною клімату, як факторів впливу на майбутній розвиток безпеки.

На основі цього, розвиток енергетичного сектору в Україні залишається на порядку денному НАТО, з часу коли виникла необхідність більш тісної співпраці з цього питання. Ряд обставин особливо цікаві у розрізі безпеки.

Енергетична безпека в рамках Особливого Партнерства між НАТО і Україною
Але перед тим як обговорити деякі елементи зі змістовної точки зору, дозвольте мені коротко згадати двосторонню програму між НАТО і Україною і що вона пропонує з точки зору енергетичної безпеки та гібридної війни.

Співпраця між Україною та НАТО базується на основі Хартії про Особливе Партнерство в 1997 році. У Статуті перераховуються загальні принципи, напрямки консультацій та співпраці, а також утверджено Комісію НАТО-Україна, яка може зустрічатися на вищому рівні Міністрів, Послів, або Комітету. Протягом тривалої кризи, ми широко використовували цей формат для проведення консультацій щодо ситуації в сфері безпеки в Україні, щоб висловити солідарність з Україною, а також прийняти рішення щодо конкретних практичних заходів, спрямованих на допомогу Україні, для кращої можливості забезпечення власної безпеки.

Програма також включає енергетичну безпеку і гібридну війну. Суттєво, що наші представники отримували системні розяснення від генерального директора НАК «Нафтогаз», Андрія Коболєва. Ми розуміли проблематику та хід перемовин між Україною, Росією та Європейською Комісією щодо «зимових пакетів» поставок газу в Україну, про прогрес, досягнутий щодо поставки природного газу в Україну через «реверсний потік», а також реформи газового ринку в Україні і «Нафтогазу». Вони також дискутували з президентом «Енергоатом» Юрієм Недашковським. Альянс і далі буде продовжувати діалог в рамках Комісії НАТО-Україна стосовно розвитку енергетики із залученням безпеки та енергетичної політики.

Енергетика також є важливим питанням для щорічної Національної програми України. Річна національна програма є привілейованим інструментом для України з метою сприяння діалогу з НАТО щодо встесторонніх державних реформ в Україні. Для союзників, це є ключовим інструментом визначення

глибини їх взаємодії з Україною. Це набагато ширше, ніж специфічна сфера компетенцій Альянсу, що охоплює політичні та економічні питання, включаючи безпеку та оборону, а також бюджетні та правові питання. Коли союзники оцінюють прогрес у його реалізації до кінця календарного року, вони проявляють особливий інтерес в політичних і економічних аспектах, які охоплюють реформи конституції, децентралізації, судової системи, боротьби з корупцією, прав людини, економічних реформ і реформи енергетичного сектора. Це показує, що ми обговорюємо питання розвитку енергетики в Україні не тільки з огляду наслідків порушення безпеки, але і тому, що «успіх цих широкомасштабних реформ матиме вирішальне значення в закладанні фундаменту процвітаючої і мирної України, міцно пов'язаної з європейськими демократіями, що віддані спільним цінностям», як це було зазначено в спільній заяві міністрів закордонних справ в Комісії НАТО-Україна в травні 2015 року.

Економічна безпека є одним з напрямків консультацій і співпраці, які були перераховані в «Хартії про особливе партнерство» вже в 1997р. У 1999 році був створений спеціалізований орган, Об'єднана робоча група з питань економічної безпеки, як майданчик для обговорення таких питань, як макроекономічний розвиток, військова економіка, а також питання енергетики. В даний час ми обговорюємо відновлення діяльності цієї групи і частині проблематики енергетичної безпеки. В ідеалі, це буде не просто майданчик для обговорення, зусилля зосереджуватимуться також на подальшій практичній діяльності, яка може бути виконана у тому числі, в рамках співпраці з Центром передового досвіду з питань енергетичної безпеки. Також зусилля спрямовуватимуться на ефективну реалізацію практичних програм, які доступні в Україні, в тому числі «Програма професійного розвитку», «Розбудова цілісності», «Наука заради миру та безпеки» та інші.

Енергетична безпека

Тепер дозвольте мені перейти до останньої частини мого виступу - енергетичних проблем, з якими стикається Україна. На підставі того, що я сказав про перспективу НАТО з питань енергетики та енергетичної політики в Україні, я хотів би виділити ряд питань, які становлять особливий інтерес для союзників і які вони, можливо, побажають обговорити з Україною.

По-перше, це досвід України щодо економічних засобів примусу і з тим, що називають енергетичним компонентом гібридної війни. Енергетика лежить в основі і навколо нинішньої кризи України: російська загроза переривання поставок газу, суперечки щодо цін, штрафів, боргів, а також активів, незаконно вилучених Росією в Криму і на Чорному морі, питання про постачання енергоресурсів в Крим і Донбас, майбутній транзит газу в Європу, поставки вугілля до українських електростанцій, безпека критично важливої енергетичної інфраструктури та багато інших.

Ці питання становлять великий інтерес і повинні бути проаналізовані, щоб краще зрозуміти роль енергетики в гібридних сценаріях війн. Деякі з цих елементів не є новими, але застосовувались Росією протягом багатьох років, і, як я вже говорив на самому початку, зумовлюють посилення інтересу НАТО в забезпеченні енергетичної безпеки. У нинішніх умовах, ці події явно виходять поза рамками визначення «енергетична безпека», оскільки є частиною гібридної стратегії дестабілізації України, і в кінцевому підсумку спровокувати крах українського уряду або навіть української держави.

Вразливість України до гібридних загроз в сфері енергетики вже давно очевидні, і її стійкість, щоб протистояти їм була порушена через невдачі власної внутрішньої політики України. Енергетика занадто довго була тим питанням, що підривало суверенітет України та перешкоджало її процвітанню. Давайте не будемо забувати, що торгівля і транзит газу були в основі руйнівних корупційних схем, заснованих на різниці цін між придбаного в Росії і виробленого в Україні газу, і газу, реалізованого кінцевими споживачами в Україні та доставленому транзитом до Західної Європи. Ці схеми мали кілька великих бенефіціарів, в Україні, в Росії, і в інших місцях, і вони мали одну головну жертву – українську державу, платників податків і стійкість економіки України.

При відсутності політичної волі для реформування економіки, диверсифікації енергопостачання та підвищення енергетичної ефективності, залежність України від імпорту енергоносіїв стало основним тягарем для її процвітання і незалежності. Харківські угоди, підписані Віктором Януковичем у 2010 році, є прикладом загроз національному суверенітету, що і мала на увазі та політика.

Енергетичні реформи є найбільш ефективним способом протистояти гібридним загрозам в енергетичній галузі. Наступні задачі реформи мають особливо важливе значення:
Створити конкурентоспроможний, ефективний і прозорий енергетичний ринок, шляхом демонополізації сектора, введення ринкових тарифів на енергетику та скасування субсидій.
Диверсифікувати джерела і маршрути поставок, щоб зберегти роль України в якості основної транзитної країни, на основі, знову ж таки прозорих і ринкових механізмів.
Розвивати внутрішнє енергопостачання, шляхом надання стимулів для інвестицій в енергетичному секторі України. Україна має значні енергетичні ресурси та потенціал, щоб стати самодостатньою.
І підвищити енергоефективність.

Багато що вже було досягнуто. Був прийнятий новий закон щодо газу. Ведеться робота по реалізації його на практиці. Україна готується до розмежування видів діяльності НАК «Нафтогаз». Підзвітність деяких великих енергетичних компаній

з державною участю була покращена. Домашні господарства отримали стимули для скорочення споживання енергії. Тарифи на електроенергію були підвищені, з наданням допомоги чутливій групі споживачів. Потужності реверсного потоку були збільшені, що дозволяє Україні купувати газ з країн ЄС.

Загалом, багато було досягнуто Україною за допомогою міжнародних партнерів, зокрема Європейського Союзу, ЄБРР і МВФ. Але багато ще належить зробити.

Союзники НАТО прагнитимуть обговорити прогрес реформ в рамках Щорічної національної програми та Комісії НАТО-Україна. І вони будуть зацікавлені, щоб обговорити з Україною досвід гібридної війни, в тому числі її енергетичну складову.

І крім того, НАТО буде продовжувати підтримувати Україну, її суверенітет і територіальну цілісність, а також її право вирішувати своє власне майбутнє і курс зовнішньої політики вільної від зовнішніх загроз. Тому що Українська незалежність, суверенітет і стабільність, її прихильність до демократії і верховенства права, і її енергетична безпека, є ключем до Євроатлантичної безпеки в цілому.

Олександр Суходоля,
завідувач відділу енергетичної та техногенної безпеки
Національного інституту стратегічних досліджень

Енергетична інфраструктура: інструментальний вибір ведення війн нового покоління

Протягом кількох останніх декад розвитку людства спостерігається ряд тривожних тенденцій, що свідчать про необхідність суттєвого переосмислення систем безпеки як на міжнародному, так і національному рівні.

Посилення екстремізму, тероризму, небувалий ріст організованої злочинності, у т.ч. міжнародної, є однією з найбільш очевидних тенденцій, що суттєво ускладнює формування безпекової політики окремих країн та посилює загрози міжнародній безпеці. Іншою тенденцією є поступове розмивання раніше чіткої межі між станом війни та станом миру, класичних методів ведення війн та розширення використання інструментів політичного та економічного тиску, інформаційного протиборства та психологічного маніпулювання.

Фактично людство опинилось у ситуації знецінення існуючих до цього часу систем забезпечення міжнародної безпеки та суттєвого ослаблення національних систем безпеки (що власне планомірно здійснювалось з огляду на створення міжнародних безпекових систем). При цьому, війни нового покоління стали вестись не стільки з огляду на нанесення поразки армії противника, скільки нанесення поразки суспільству, яке утримує армію, через руйнування інфраструктури життєдіяльності цього суспільства та функціонування економіки та держави.

В умовах глобалізації економіки та торгівлі, об'єднання транспортних мереж, а також порушення міжнародної системи безпеки знищення інфраструктури життєдіяльності суспільства може навіть виступати інструментом опосередкованого впливу одних країн на інші, навіть на країни які непричетні до конфлікту. Прикладом цього є міграційний потік з країн охоплених війною (Сирії, Іраку, Афганістану) до країн ЄС.[1]

Динаміка взаємовідносин України та Росії у енергетичній сфері у передвоєнний період, а також проблеми забезпечення функціонування енергетичної інфраструктури у 2014-2015 роках, яскраво відображає можливості використання Росією енергетичного сектору у якості інструменту політики зовнішньої політики підкорення України.

---

[1] Туск: хвиля біженців - новий інструмент в гібридній війні. [Електронний ресурс]. – Режим доступу: http://www.polradio.pl/5/38/Artykul/223774.

1. «Енергетична зброя» мирного часу

Використання енергетичного сектору як «енергетичної» зброї було відкрито проголошене у 2003 р. в Енергетичній стратегії Російської Федерації до 2020 р., де зазначалося, що потужний паливно-енергетичний комплекс Росії «є базою розвитку економіки, інструментом здійснення внутрішньої та зовнішньої політики». Яскравим прикладом такої політики може слугувати передусім сфера газопостачання, яка виступала інструментом досягнення політичних цілей Росії у взаємовідносинах із Україною та країнами Європейського Союзу.
Даний інструмент широко використовувався Росією протягом тривалого часу не тільки шляхом нав'язування невигідної економічної моделі взаємовідносин із країнами партнерами, але й через пошкодження енергетичної інфраструктури.

Даний аспект неодноразово відзначався фахівцями у сфері енергетики, хоча більшість західноєвропейської політичної еліти та галузевих експертів, бажаючи залишитись у дружніх стосунках із важливим постачальником енергоресурсів, намагались розглядати поведінку Росії виключно в межах економічної раціональності.

Для України ж, як і для інших країн колишнього СРСР, застосування Росією енергетики, у якості інструменту обмеження суверенітету було реальністю. Фактично, історія відносин між Україною та Росією в енергетичній сфері була перманентною «прихованою» війною між бажанням України отримати незалежність та бажанням Росії зберегти Україну у сфері свого політичного, економічного та технологічного впливу.

Росія, у якості інструментів підпорядкування застосовувала: монополізацію ринку країни споживача за допомогою маніпулювання цінами (надання знижок окремим компаніям та країнам за укладання довгострокових контрактів); корумпування посадових осіб кран споживачів та менеджерів компаній (укладання контрактів на вигідних для Росії умовах); недопущення формування спільного ринку країн споживачів (перешкоджання формування спільного ринку країн споживачів, заборона на реекспорт енергоносіїв в рамках угод з Росією, надання переваг окремим країнам (компаніям) у доступу до внутрішнього ринку Росії).

Найбільш очевидним проявом такої політики Росії по відношенню до України є використання вищезазначених інструментів, які зумовили укладання невигідних контрактів на постачання природного газу у 2009 році, наступний обмін знижки на вартість природного газу на продовження терміну довгострокової оренди Чорноморського Флоту Росії в Україні у 2010 році, відмова від укладання угоди про Асоціацію між Україною та ЄС взамін на уникнення штрафів за невиконання контрактів 2009 року та надання додаткових кредитів на закупівлю газу у 2013 році.[2]

[2] Суходоля О.М. Трансфер досвіду як інструмент аналізу політики // Науковий вісник Академії муніципального управління. – 2013. – № 2. – С. 66–80.2014. – № 4. – С .5-12.

У якості прикладів використання енергетичної інфраструктури для досягнення окремих цілей відмітимо наступні випадки: майже синхронні підриви енергетичної інфраструктури, які припинили постачання природного газу та електроенергії до Грузії у січні 2006 р.; вибух на газопроводі у Туркменістані у квітні 2009 р.; зупинка у 2006 р. на ремонт нафтопроводу, який забезпечував постачання нафти на нафтопереробний завод у Мажейкяй у Литві.[3]

На нашу думку, саме нехтування світовим співтовариством спроб Росії використовувати енергетику у якості зброї у міжнародних відносинах у попередній період, сприяло імплементації енергетичного виміру в нову концепцію ведення війн. Розпочавши агресію Росія просто змінила акцент дій проти України з економічного виснаження економіки, через укладання невигідних угод в напрямку фізичного впливу, на пошкодження функціонування енергетичної інфраструктури.

2. Пошкодження енергетичної інфраструктури як метод ведення війни

Енергетика та енергетична інфраструктура стали важливими цілями Росії під час анексії Криму та захоплення окремих районів Луганської та Донецької областей у 2014-2015 роках.

Цілі у сфері енергетики полягали не тільки у захопленні енергетичних активів але й у цілеспрямованому пошкодженні енергетичної інфраструктури. Попередній аналіз випадків пошкодження інфраструктури у 2014-2015 роках,[4] свідчить про те, що порушення енергетичної інфраструктури використовувалось для підриву стабільності соціально-економічної ситуації в країні та легітимності новоутвореного уряду України.

У загальному випадку, аналіз випадків пошкодження функціонування критичної енергетичної інфраструктури, в умовах ведення війни виділяє дві основні групи дій:

- **дії без цільового наміру**, де порушення функціонування інфраструктури є своєрідним «побічним» наслідком збройного протиборства, зокрема неточність обстрілів при веденні бойових дій.
- **цілеспрямовані дії суб'єкта** спрямовані на порушення спроможності енергетичної інфраструктури виконувати свої функції, які, у свою чергу, розділимо за ступенем руйнівного впливу:

[3] В.П. Горбулін. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу // Стратегічні пріоритети 2014. – № 4. – С .5-12.

[4] Суходоля О.М. Проблеми захисту енергетичної інфраструктури в умовах гібридної війни. [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/1891/

- фізичне захоплення об'єктів при збереженні їх функціональності (змінюється лише отримувач ренти від їх функціонування)[5];
- припинення функціонування об'єктів, у тому числі внаслідок фізичного захоплення, для нанесення збитків попередньому власнику чи обміну на «потенційні» переваги в інших сферах (задоволення політичних вимог, викуп, вплив на ринкову вартість тощо)[6];
- розукомплектування окремих елементів інфраструктури з метою отримання доходу від їх продажу (металобрухт) [7];
- фізичне знищення об'єкта (його функціональної спроможності), для нанесення критичної шкоди як в частині збільшення витрат противника на переборення стану порушення функціонування інфраструктури (наприклад, неможливість доставити ресурси), так і формування суспільно-політичного невдоволення населення країни;[8]
- перешкоджання діяльності з віднновлення функціональності енергетичної інфраструктури.[9]

Окремим методом цілеспрямованого зловмисного впливу на функціонування енергетичної інфраструктури слід вважати здійснення кібератак, спрямованих на втручання в роботу систем технологічного управління. Прикладом цього стала перша у світі хакерська атака проти енергетичної системи, здійснена наприкінці 2015 року групою хакерів з Росії.

---

[5] Зокрема захоплення об'єктів енергетики у Криму та плани захоплення компресорних станцій магістральних газопроводів, які за планами Генштабу РФ треба захопити і не руйнувати. Детальніше: «Геращенко розповів про плани Генштабу РФ захопити Лівобережну Україну за 15 днів». [Електронний ресурс]. – Режим доступу: http://www.unian.ua/politics/1089884-geraschenko-rozpoviv-pro-plani-genshtabu-rf-zahopiti-livoberejnu-ukrajinu-za-15-dniv.html

[6] Наприклад, через дефіцит антрацитового вугілля, що видобувається переважно на окупованій території Донбасу, виникла загроза зупинки половини українських теплових електростанцій, частини теплоелектроцентралей і котелень, що загрожувало стабільності енергозабезпечення всієї країни. Дана ситуація, фактично змусила Україну йти на поступки в питанні енергопостачання Криму, закупівель газу чи свого ж вугілля у Росії, фактично фінансуючи війну.

[7] Село Троїцьке (Луганська обл.) у червні 2015 року залишилось без світла, внаслідок обстрілів, проте відновити електропостачання не вдавалось із-за того, що трансформатори були порізані на металолом місцевими жителями. Явище мародерства, розукомплектування об'єктів енергетики та їх продажу на металобрухт набуло неймовірного розмаху на сході України. У «ДНР» навіть створили окреме «Державне підприємство «Вторчормет», яке масова здійснювало продаж металобрухту. Мобільні бригади на «Газелях» із встановленими різаками металу пиляють усе, від кабелів і рейок до цехів підприємств. [Електронний ресурс]. – Режим доступу: http://gazeta.dt.ua/macrolevel/blokada-bezgluzda-y-neschadna-_.html.

[8] Боевики умышленно взорвали газопровод, снабжающий Мариуполь – МВД. [Електронний ресурс]. – Режим доступу: http://news.liga.net/news/politics/5983963-boeviki_umyshlenno_vzorvali_gazoprovod_snabzhayushchiy_mariupol_mvd.htm

[9] У червні 2015 року жителі міста Красногорівки та сусідньої з нею Мар'їнки в Донецькій області більше двох тижнів жили без електроенергії та мали проблеми з водопостачанням (через зупинку насосів). Снайпери з боку ДНР стріляючи по електриках не допускаючи їх до виконання ремонтних робіт. Обстріли бригад які відновлювали газопостачання Красногорівки здійснювались і у 2016 році.

Кібератака спричинила відключення енергопостачання у шести розподільчих енергокомпаніях та мала комплексний характер та складалась як мінімум з таких складових: попереднє зараження мереж; захоплення управління АСДУ з виконанням операцій вимикань на підстанціях; виведення з ладу елементів ІТ інфраструктури; знищення інформації на серверах та робочих станціях; відмови в обслуговуванні знеструмлених абонентів. У результаті без електропостачання залишилися 103 населені пункти України. Перерва в електропостачанні склала від 1 до 3,5 годин. [10]

У загальному випадку дії спрямовані на порушення функціонування енергетичної інфраструктури сприяли:

- **здійсненню психологічного тиску,** через створення інформаційних приводів з метою поширення панічних настроїв, соціальної напруги та невдоволення керівництвом країни;
- **нанесенню економічних збитків** через захоплення енергетичних об'єктів й ресурсів та необхідності додаткових витрат на відновлення інфраструктури та додаткових поставок ресурсів;
- **отриманню локальних переваг**, як то досягнення кращої позиції у проведенні окремих операцій (бойові зіткнення, контрактні умови, чи мирні переговори), примушування здійснення окремих дій (платежів, продажу чи закупівлі ресурсів) чи вилучення доступних для ресурсів;
- **формуванню необхідного «іміджу» на міжнародній арені**, як то створення негативного іміджу України у випадку припинення енергопостачання Криму чи активна пропаганда допомоги В.Путіна у постачанні природного газу до Геніческа після «фейкового» звернення мера міста.

[10] Міненерговугілля має намір утворити групу за участю представників усіх енергетичних компаній, що входять до сфери управління Міністерства, для вивчення можливостей щодо запобігання несанкціонованому втручанню в роботу енергомереж. [Електронний ресурс]. – Режим доступу: http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245086886&cat_id=35109

Таблиця 1. Використання енергетики у якості інструменту ведення війни
(на прикладі подій 2014-2015 років в Україні)

здійснення психологічного тиску	**нанесення економічних збитків**	**отримання локальних переваг**	**формування необхідного «іміджу»**
Загроза порушення сталого функціонування об'єднаної енерге-тичної системи країни (*внаслідок відсутності палива (вугілля, природного газу) для електростанцій*) Припинення енергопостачання населених пунктів (пошкодження *ТЕС та трансформа-торних підстанцій регіону, підрив газопроводів для Маріуполя, Бердянська*); Припинення водопостачання населених пунктів внаслідок знеструмлення насосних станцій (*пошкодження електропостачання, пошкодження трубопроводів, перешкоджання ремонтним роботам*)	Захоплення об'єктів та інфраструктури в Криму (*підприємств, родовищ, інфраструктури*); Примушування до оплати товарів (послуг) (*оплати природного газу та електроенергії на окуповану територію, за яку споживачі цих територій не сплачують*) Продаж під виглядом російського вугілля, *захопленого на окупованій території*;	Захист від можливих атак (*розміщення військових підрозділів на територіях які небезпечно атакувати - хімічних заводів чи мереж енергопостачання (розміщення бойових позицій побли-зу магістральних газопроводів)* Створення переваг у військових операціях (*неможливість залишення об'єктів інфраструктури підрозділами захисту, як то електростанцій, транспортних вузлів, аеропортів, компресорних та насосних станцій*)	Отримання переваг у політичному переговорному процесу (*забезпечення кращої політичної позиції у переговорному процесі)* Створення тиску з боку інших країн (*формування бажаного іміджу (позитивного для Росії та негативного для України) на міжнародній арені, - на прикладі критики щодо припинення Україною енергопостачання Криму, надання гуманітарної з боку Росії, примушування до фінансування захоплених Росією територій*)

Аналіз подій щодо цілеспрямованого руйнування інфраструктури життєдіяльності свідчить про формування нового типу ведення війни – «інфраструктурної війни». Специфіка такого типу війни визначається її метою, а саме підпорядкування країни не стільки через завдання поразки її збройним силам, скільки через повалення уряду країни, деморалізацію суспільства та формування хаосу управління та функціонування економіки цієї країни, за допомогою цілеспрямованого погіршення умов життєдіяльності населення та формування незадоволення владою з боку місцевого населення.

Причиною того, що пошкодження чи знищення критичної енергетичної інфраструктури стає таким критичним стало неймовірне зростання залежності людини від цієї інфраструктури. Порушення «звичних умов існування» може сформувати невдоволення населення країни своїм керівництвом, а відтак основою соціально-політичних протестів проти влади. При цьому, енергетична інфраструктура є визначальною, оскільки саме завдяки їй (насамперед інфраструктура електропостачання) вся інша критична для життєдіяльності людини, суспільства та держави інфраструктура спроможна виконувати и свої функції.

Загалом ефективність «цілеспрямованого, зловмисного» пошкодження енергетичної інфраструктури країни, залежить від різноманітних чинників, серед яких, у якості головних, слід виділити:

- рівень самозабезпечення споживачів та спроможність до відновлення функціонування інфраструктури;
- чутливість людини (суспільства) до порушення енергозабезпечення.

Рівень самозабезпечення енергопостачання є своєрідною технічною вимогою розвитку інфраструктури, що пов'язується передусім із спроможністю енергетичної інфраструктури оперативно відновлювати свої функції, а на практиці реалізується шляхом застосування ряду організаційно-технічних заходів (фізичний захист, резервні потужності та мережі, диверсифікація джерел та маршрутів постачання, тощо), завчасно підготовлених у мирний період на випадок кризових ситуацій.

Чутливість же людей до порушення енергозабезпечення, на наш погляд, визначається позиціюванням людини (територіальної громади) щодо країни. Дане позиціювання можливо описати через складові: «звичні умови існування» людей та їх «національна ідентифікація».

«***Звичні умови існування***» визначатимуть ту ступінь пошкодження інфраструктури життєдіяльності, яку населення окремої території вважатиме недопустимим, а у випадку його досягнення буде готове відмовити уряду у легітимності. Очевидно, що «звичні умови існування» населення міст Баварії та Донбасу відрізнятимуться, як і рівень їх «згоди» на обмеження енергопостачання.

«***Національна ідентифікація***» визначатиме ступінь готовності жителів окремих територій враховувати інтереси всієї країни. Очевидно, що відсутність ідентифікації себе з країною визначатиме небажання населення зносити обмеження енергопостачання та формуватиме готовність до звинувачення влади у їх проблемах.

Поєднання цих двох чинників пояснює «згоду» населення окупованих територій на пошкодження інфраструктури, оскільки вони «звичні» до випадків обмеження енергозабезпечення, а відсутність прив'язки до української держави зумовлювали готовність звинувачувати українську владу з будь-якого приводу (навіть якщо порушення інфраструктури спричинене з боку агресора).[11]

У загальному це дає підстави сформувати наступну гіпотезу: ***порушення інфраструктури енергозабезпечення для країн із високим рівнем технологічної залежності життєдіяльності суспільства є ефективним інструментом послаблення країни та підтримки агресора населенням, яке не ідентифікує себе з цією країною.***

3. Заходи запобігання пошкодження енергетичної інфраструктури

Аналіз подій у сфері функціонування енергетики України під час війни у 2014-2015 роках дозволяє також визначити заходи, які можуть застосовуватись для зниження ризиків припиненню функціонування енергетичної інфраструктури, зокрема:

- проведення роз'яснювальної роботи із населенням, збройними та правоохоронними силами щодо важливості забезпечення функціонування критичної енергетичної інфраструктури;
- застосування «плану реагування», тобто застосування правоохоронних та збройних сил у наперед визначених заходах попередження захоплення та захисту критичної енергетичної інфраструктури при досягненні визначеного рівня загроз (терористичних актів);
- формування ресурсів та засобів мобільного енергозабезпечення населених пунктів, використання технічних можливостей збройних сил;
- запровадження додаткових організаційно-технічних заходів захисту критичної інфраструктури від випадкових пошкоджень;
- формування системи комунікацій між ворогуючими сторонами, із залученням представників конфлікту та незацікавленої сторони;
- встановлення тимчасового локального перемир'я між ворогуючими сторонами (для проведення робіт з відновлення систем електро-, газо-, , та водопостачання);
- запровадження міжнародного моніторингу (залучення третьої сторони), з метою недопущення цілеспрямованого пошкодження інфраструктури конфліктуючими сторонами та перешкоджання відновленню інфраструктури ремонтними бригадами;
- уникнення розміщення воєнних формувань (центрів управління) на території чи поблизу критичної енергетичної інфраструктури;
- координація захисту енергетичної інфраструктури у місцях бойових

[11] Звинувачення у всіх проблемах українську владу активно підтримувалось засобами інформаціно-психологічної підтримки дій нової влади здійснювалось з боку Росії, у тому числі шляхом провокацій.

зіткнень між збройними силами та правоохоронними органами, з метою недопущення мародерства;

- асиметричне використання «енергетичного виміру» відносно територій агресора (окупованих агресором територій); [12]

Всі розглянуті заходи, передбачають формування спроможності держави запобігати виникненню кризової ситуації внеслідок здійснення «цілеспрямованих, зловмисних дій» проти енергетичної інфрастуктури. Інструментами запобігання виникнення криз можуть виступати інженерно-технічні, охоронні заходи, політичні домовленості та використання міжнародної правової бази.

При цьому заходи запобігання пошкодження інфраструктури або оперативного відновлення її функціонування у період війни, базуються на (та слугують лише допоміжним елементом) загальнодержавній системі захисту критичної енергетичної інфраструктури сформованої для мирного часу, однак побудованій на «проактивній» методології.

4. Створення системи захисту енергетичної інфраструктури

Пріоритетним напрямом безпекової політики держави є підвищення рівня безпеки та стійкості енергетичної інфраструктури стосовно всього спектра загроз і ризиків. Метою захисту є забезпечення безперебійного сталого функціонування інфраструктури, запобігання її руйнуванню, та забезпечення швидкого відновлення функціонування після збою в роботі.

Принципова відмінність пропонованої системи захисту від наявної системи цивільного захисту полягає в її цільовій спрямованості. Метою системи захисту критичної енергетичної інфраструктури є гарантування спроможності інфраструктури виконувати передбачені функції (надавати послуги), а не захист населення й довкілля від наслідків надзвичайних ситуацій, що є головним завданням системи цивільного захисту. Фактично ідеться про зміщення фокусу уваги на попередження кризових ситуацій, пов'язаних із функціонуванням КІ.

Загальним підходом до формування системи захисту є запровадження системи оцінювання ризиків формування кризових ситуацій як на рівні держави, так операторів інфраструктури, а також планування й здійснення заходів недопущення їх реалізації, що формалізується в рамках «превентивного планування».

---

[12] Припинення постачання електроенергії до Криму з боку України дозволило: у березні 2014 року забезпечити формалізацію стосунків, підвищення цін та оплату за спожиту електроенергії з боку споживачів Криму на адресу українських виробників; у грудні 2014 року забезпечення розрахунків, погодження на тимчасові обмеження у енергопостачанні та розблокування постачання вугілля для електростанцій України з боку Росії (з 24 листопада 2014 року постачання вугілля з Росії було заблоковано); 24 та 26 грудня тимчасово припинялось постачання електроенергії в Крим; 26 грудня постачання вугілля (1000 вагонів вугілля було заблоковано на кордоні) та електроенергії з Росії в Україну було відновлено (без передоплати та по внутрішнім цінам); у червні 2015 року для забезпечення розрахунків.

Стосовно енергетичної інфраструктури, прикладом такого підходу у Європейському Союзі, є запровадження Регулювання ЄС №994/2010 щодо заходів забезпечення безпеки газопостачання,[13] що вимагає від національних урядів розробити «План попередження криз» (Preventive Action Plan) та «План реагування на кризи» (Emergency Plan) у сфері газопостачання.

«План попередження криз» має містити заходи для усунення або пом'якшення ризиків, зокрема передбачати наявність:

- оцінки ризиків (у відповідності до встановленої методології);
- засобів, обсягів, та потужностей спроможних вчасно компенсувати пошкодження найбільшого елементу інфраструктури та забезпечити стандарти постачання (відповідно до встановлених вимог);
- зобов'язань що накладаються на операторів або відповідних служб, включаючи вимоги щодо безпеки функціонування інфраструктури;
- інші запобіжні заходи, такі як підвищення взаємопов'язаності інфраструктури та можливості забезпечити диверсифікації постачання (джерел та маршрутів);
- механізмів співпраці із постачальниками інших країн (регіонів);
- інформування щодо існуючих та будівництва майбутніх міжсистемних зав'язків (інтерконекторів), що забезпечує перетоки між системами на випадок виникнення кризових ситуацій;

«План реагування на кризи» має містити заходи забезпечення належного функціонування системи газопостачання відповідно до рівня кризової ситуації (раннього попередження (early warning); оповіщення ризику (alert); аварійна ситуація (emergency)), [14] зокрема:

- визначення ролі та відповідальності операторів газопостачання та промислових споживачів та їх взаємодію із відповідними органами влади у випадку виникнення кризових ситуацій у відповідності до встановлених рівнів;
- визначення ролі та відповідальності відповідних органів влади та інших

---

[13] Regulation (EU) No 994/2010 of the European Parliament and of the Council of 20 October 2010 concerning measures to safeguard security of gas supply and repealing Council Directive 2004/67/EC Text with EEA relevance

[14] Для цілей запровадження системи захисту критичної інфраструктури в Україні пропонується виділення наступних режимів її функціонування:

- стале функціонування – КІ функціонує в нормальному режимі (ринкових умовах), обмеження щодо економічної діяльності чи правового регулювання не запроваджуються, здійснюється моніторинг загроз;
- попередження кризових ситуацій – КІ функціонує в стані готовності до застосування чи вжиття окремих заходів, проте без обмежень щодо економічної діяльності чи правового регулювання, здійснюється моніторинг загроз та оцінка ризиків, застосовуються ресурси й сили, передбачені об'єктовою проектною загрозою без залучення зовнішніх сил;
- діяльність в умовах кризової ситуації – КІ функціонує в умовах обмежень, запроваджуються особливі режими економічної діяльності й правового регулювання, здійснюється реагування на ризики припинення функціонування із залученням зовнішніх сил і ресурсів;
- функціонування в режимі надзвичайного чи воєнного стану – КІ функціонує в особливих умовах, визначених окремими законами;

служб відповідно до задач визначених планом реагування на кризові ситуації відповідно до їх рівня;

- забезпечення спроможності операторів та споживачів, відреагувати на кризові ситуації відповідно до їх рівня;
- визначення заходів та дій необхідних для пом'якшення негативного впливу припинення газопостачання на інші системи життєзабезпечення;
- встановлення детальної процедури та заходів, які необхідно задіяти за різними рівнями кризових ситуацій, включаючи схему взаємодії та обміну інформацією;
- запровадження «кризового менеджера», визначення його ролі та повноважень;
- визначення внеску неринкових заходів, які мають застосовуватись на етапі кризової ситуації (наперед визначений перелік);
- формування механізму забезпечення співпраці між країнами за різними рівнями кризової ситуації;
- надання детального переліку вимог до діяльності операторів газопостачання на етапі оповіщення ризику та аварійної ситуації;
- встановлення переліку наперед визначених дій щодо гарантування газопостачання у кризовій ситуації.

Розглянуті проблеми та пропоновані удосконалення системи захисту критичної енергетичної інфраструктури, потребують свого відображення у всій системі державного управління. Дане завдання можливо врегулювати шляхом запровадження окремого документу, який визначить загальні підходи та механізми забезпечення захисту критичної енергетичної інфраструктури.

Саме таким документом, який формує засади системи захисту критичної інфраструктури, виступає «Зелена книга із захисту критичної інфраструктури», концептуальні положення якої розроблені Національним інститутом стратегічних досліджень.[15]

[15] Зелена книга з питань захисту критичної інфраструктури/ Автори: Бірюков Д.С., Кондратов С.І., Насвіт О.І., Суходоля О.М. [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/public/File/2015_table/Green%20Paper%20on%20CIP_ua.pdf.

Дмитро Бірюков,
завідувач сектору
Національного інституту стратегічних досліджень

Захист критичної інфраструктури: новий вимір безпекової політики України

Питання захисту критичної інфраструктури стає вкрай актуальним для України в умовах нинішнього безпекового середовища. Ця актуальність обумовлена як значимістю інфраструктури для забезпечення життєдіяльності суспільства, розвитку національної економіки, здійснення державного управління, так і зростанням рівня загроз для об'єктів інфраструктури в умовах здійснення проти України агресії ззовні.

Сам термін «критична інфраструктура» вже є зрозумілим та навіть звичним для вітчизняних теоретиків і практиків з питань забезпечення національної безпеки. Зростання інтересу до нього в «експертному середовищі» пов'язано з низкою процесів, що останніми роками розвиваються паралельно.

По-перше, значно зросла кількість випадків, які можна назвати реалізацією загроз об'єктам критичної інфраструктури (процес практичного протистояння загрозам), переважно викликаних веденням проти Української держави гібридної війни. Тут, насамперед, можна згадати диверсійно-терористичну діяльність в східних регіонах і кібератаки на енергетичні мережі (грудень 2015р.).

По-друге, термін «критична інфраструктура» все частіше з'являється в національних нормативно-правових документах (процес формалізації), зокрема, Стратегії національної безпеки, рішенні Ради національної безпеки і оборони, Зеленій книзі[16], Концепції розвитку сектору безпеки і оборони, Стратегії кібербезпеки, а також в низці законопроектів. Тут слід відмітити піонерську роль НІСД з «популяризації» концепції захисту критичної інфраструктури як елементу системи забезпечення національної безпеки та пошук шляхів її імплементації (див. огляд в [17, с. 155-170, с. 116-131]).

По-третє, реформування сектору безпеки і оборони підвищило інтерес до вивчення підходів, що запроваджені в країнах учасницях НАТО та країнах ЄС (процес інституційного реформування). І останнє, критична інфраструктура є багатообіцяючим об'єктом наукового дослідження в різних галузях знань (зокрема, економіка, політологія, державне управління, воєнні науки та національна безпека, комп'ютерні науки та інформаційні технології), а часто і міждисциплінарних досліджень. Наприклад, вітчизняні науковці неодноразово

---

[15] Зелена книга з питань захисту критичної інфраструктури розроблена в НІСД на виконання завдання, зазначеного у п. 2.1.4 Річної національної програми співробітництва Україна – НАТО на 2015 рік (затверджена Указом Президента України від 23 квітня 2015 р. № 238/2015)

[16] Науково-інформаційний вісник Академії національної безпеки. – 2015. – № 3-4 (7-8).

зверталися до вивчення питань кібер-безпеки об'єктів критичної інфраструктури, її організаційного та правового забезпечення.

Тут слід згадати серію конференцій, яку організовувала Національна академія Служби Безпеки України, роботи які обговорювалися на цих заходах, зокрема, щодо захисту інформаційної інфраструктури в контексті контррозвідувального забезпечення інформаційної безпеки держави [18, с.28-33], категоризації об'єктів у оборонній сфері [19, с.194-198], оцінки деструктивного інформаційного впливу на об'єкти критичної інформаційної інфраструктури [20, с.221-223]. Потрібно також окремо відмітити роботи *В. Панченко*, яка досліджувала зарубіжний досвід формування системи захисту критичної інфраструктури від кібер-загроз [21], *В. Петрова* щодо політики держав Східного партнерства в даній сфері [22], а також дослідження проблем управління національною інформаційно-комунікаційною інфраструктурою, здійснене *С.Рибкою, Є.Кільчицьким, О.Післегіним* [23].

Про те, що *захист критичної інфраструктури стверджується як елемент державної безпекової політики*, свідчить присутність в Стратегії національної безпеки України з-поміж основних напрямів державної політики національної безпеки окремого пункту (п.4.13) – забезпечення безпеки критичної інфраструктури. Більш того, Стратегія з-поміж пріоритетів вирішення цього завдання називає створення системи державного управління безпекою критичної інфраструктури. Необхідність останньої обумовлена як об'єктивними факторами безпекового середовища – крайнім загостренням загроз національній безпеці, в умовах підсилення дестабілізуючих факторів ініційованих із-зовні, так і суб'єктивними – відсутність в державі цілісного механізму попередження та управління кризовими ситуаціями, пов'язаними із функціонуванням критичної інфраструктури України.

Можна побачити певну ієрархію завдань забезпечення захисту критичної інфраструктури, які вказуються в Стратегії національної безпеки, яка обумовлена взаємозалежністю між ними. Так, базовим завданням є «комплексне вдосконалення правової основи захисту критичної інфраструктури», від його виконання напряму залежить формування державної системи захисту критичної інфраструктури, а інші завдання теж мають здійснюватися на оновленій нормативно-правовій основі. Проте, слід наголосити, що це завдання досі не покладено на жодний орган виконавчої влади в Україні.

---

[18] Актуальні проблеми управління інформаційною безпекою держави: зб. матер. наук.-практ. конф., 30 березня 2012 р., м. Київ. – К. : Наук-вид. відділ НА СБ України, 2012. – 301 с.

[19] Там само.

[20] Там само.

[21] Панченко В.М. Зарубіжний досвід формування систем захисту критичної інфраструктури від кіберзагроз // Інформаційна безпека людини, суспільства, держави. – 2012. – № 3. – С. 91 – 100.

[22] Петров В.В. Політика держав Східного партнерства щодо захисту критичної інфраструктури від кіберзагроз // Стратегічні пріоритети. – 2014. – № 2. – С. 88 – 97.

[23] Рибка С.В., Кільчицький Є.В., Післегін О.М. Кіберпростір, управління інфраструктурою, кібербезпека // Стратегічна панорама. – 2015. - №1. – С. 126 – 134.

В згаданій вище Зеленій книзі представлені концептуальні елементи, що визначають етапи введення захисту критичної інфраструктури в практику державної безпекової політики (рис.2). Між цими концептуальними елементами є безпосередній взаємозв'язок. Так, стратегічні цілі державної політики визначають завдання захисту критичної інфраструктури та принципи побудови відповідної державної системи. В свою чергу останні два концептуальні елементи визначають завдання державної системи захисту критичної інфраструктури, на основі переліку яких уточнюються функції суб'єктів такої системи.

Потрібно підкреслити такі специфічні риси, що привносить **захист критичної інфраструктури** в систему забезпечення національної безпеки **в умовах протистояння агресору в гібридній війні**:

- розглядає питання *застосування спеціальних заходів* (засобів) із забезпечення безпеки і стійкості критичної інфраструктури *в умовах правового режиму мирного часу*, але із врахуванням де-факто воєнного конфлікту;
- *загрози оцінюються в комплексі* (аварії й технічні збої, природні лиха та небезпечні природні явища, зловмисні дії, зокрема, зловмисні дії груп або окремих осіб, таких як терористи, злочинці й диверсанти, промислове шпигунство, а також бойові дії) та з огляду на *вплив на національну безпеку*;
- розглядає *широкий перелік об'єктів* в різних секторах, проте *концентрується на ключових* (енергетика та ІТС).

Поряд з ними захист критичної інфраструктури привносить в практику формування та реалізації державної політики таке [24]:

- дозволяє як державі (в особі органів виконавчої влади), так і операторам критичної інфраструктури *визначати пріоритети* щодо здійснення заходів для підсилення захисту і забезпечення неперервності життєво важливих функцій для суспільства та національної економіки;
- дозволяє *перерозподіляти ресурси*, концентруючи увагу на переліку критичних об'єктів захисту та виходячи з визначених вимог до забезпечення безпеки;
- формує *партнерські стосунки* між державою та операторами критичної інфраструктури, створює *інформаційний обмін* щодо загроз;
- *стійкість та безпека* критичної інфраструктури нерозривно *пов'язується із економічним зростанням*, соціальним добробутом, технологічним розвитком тощо.

Можна відмітити певний *розвиток правових та організаційних основ*, необхідних для здійснення *державної політики щодо захисту критичної інфраструктури*, що відбувся протягом 2015 – першої чверті 2016 року. За попередній рік виділимо такі групи подій.

- *Законодавчі ініціативи.* Загальна повільність запровадження системи захисту критичної інфраструктури пов'язується, зокрема, із відсутністю

[24] Бірюков Д.С., Кондратов С.І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. – К.: НІСД, 2012. – 96 с.

законодавчого визначення термінології та основних засад державної політики у цій сфері. Частково дане питання намагались вирішити в рамках розробки законопроекту «Про основні засади забезпечення кібербезпеки України» (зареєстрований під №2126а від 19.06.2015р., відкликаний 02.02.2016р.) в рамках визначення термінів «критична інформаційна інфраструктура». Ще один законопроект, на який слід звернути увагу, – «Про внесення змін до закону України «Про інформацію» (щодо визначення норм обов'язкового захисту)» (зареєстрований під №2661 від 17.04.2015р., відхилений та знятий з розгляду 04.06.2015р.). В ньому пропонувалося доповнити Закон України «Про інформацію» статтею 191, в якій зокрема вказати: «технологічна інформація щодо об'єктів життєзабезпечення, транспортної, інформаційної та/або телекомунікаційної інфраструктури, об'єктів підвищеної небезпеки, інших об'єктів, порушення сталого функціонування яких може спричинити аварії та/або надзвичайні ситуації, негативно вплинути на стан здоров'я та безпеку людей, умови їх життя, несе підвищену небезпеку для обороноздатності держави, стану довкілля, економічної, політичної, соціальної стабільності суспільних відносин або провадження суб'єктами господарювання діяльності, підлягає захисту згідно із законодавством». Іншими словами, технологічна інформація на об'єктах критичної інфраструктури підлягає захисту, а порядок такого захисту має бути законодавчо визначений.

- *Створення координаційних органів*. В січні 2015 р. Постановою № 18 Кабінет Міністрів України затвердив Положення про Державну комісію з питань техногенно-екологічної безпеки та надзвичайних ситуацій і її склад, яка є постійно діючим органом, який забезпечує координацію діяльності центральних і місцевих органів виконавчої влади, пов'язаної із забезпеченням техногенно-екологічної безпеки, захисту населення і територій від наслідків надзвичайних ситуацій, організаційних заходів протидії терористичній діяльності та воєнній загрозі, запобігання виникненню надзвичайних ситуацій і реагування на них. Прийняття зазначеної постанови, формально, частково вирішує питання координації дій щодо захисту критичної інфраструктури, проте обмежується лише рамками надзвичайних ситуацій в розумінні системи цивільного захисту.

- *Здійснення ідентифікації об'єктів критичної інфраструктури*. В 2015 році здійснювалися певні спроби формування переліку критичної інфраструктури. Так, на селекторній нараді «з питань безпеки громадян та захисту найважливіших об'єктів інфраструктури», що проходила під головуванням Прем'єр-міністра України в січні 2015 р., Мінекономрозвитку разом із центральними та місцевими органами виконавчої влади (пункт 5 протоколу селекторної наради від 23.01.2015р. №2666/01-15) було доручено сформувати перелік об'єктів транспортної та критичної інфраструктури, а також місць масового перебування людей, які потребуватимуть першочергового захисту у разі ускладнення ситуації, у тому числі зумовленою терористичними загрозами. З метою вироблення єдиного підходу до формування такого переліку в Мінекономрозвитку були розроблені тимчасові

рекомендації щодо визначення об'єктів (направлені до відповідних центральних та місцевих органів виконавчої влади разом із формою для внесення об'єктів в перелік – фактограма від 29.01.2015 №2327-07/2835-03). Також слід згадати, що Кабінетом Міністрів України доручалося Адміністрації Держспецзв'язку розробити та подати для затвердження порядок віднесення об'єктів до критичної інформаційної інфраструктури держави, сформувати перелік таких об'єктів, організувати та провести оцінку стану захищеності державних інформаційних ресурсів зазначених об'єктів (пункт 4 Плану заходів щодо захисту державних інформаційних ресурсів, затвердженого Розпорядженням Кабінету Міністрів України від 05.11.2014 р. №1135).

- *Покращення управління в умовах кризових ситуацій*. В січні 2015 р. розпочав роботу Головний ситуаційний центр України при Раді національної безпеки і оборони України, а в структурі Апарату присутня Служба забезпечення діяльності Головного ситуаційного центру. Міністерством оборони України, яке було призначене відповідальним за розробку концепції створення ефективної державної системи кризового реагування (мережі ситуаційних центрів центральних органів виконавчої влади) та плану заходів щодо реалізації зазначеної концепції (п.3. Плану заходів з виконання Програми діяльності Кабінету Міністрів України та Стратегії сталого розвитку «Україна - 2020» у 2015 році, затвердженого розпорядженням Кабінету Міністрів України від 04.03.2015 р. № 213-р), були розроблені та надіслані до Кабінету Міністрів України пропозиції щодо проектів.

В березні 2016 року указами Президента України були введені в дію два важливих стратегічних документа: Концепція розвитку сектору безпеки і оборони України та Стратегія кібербезпеки України. В них захист критичної інфраструктури неодноразово згадується і пов'язується з вирішенням завдань в таких державних системах як цивільний захист, контррозвідувальна діяльність, кібербезпека, фізичний захист.

Тут слід зауважити, що в Концепції розвитку сектору безпеки і оборони України вперше вказується на роль контррозвідувальної діяльності в захисті критичної інфраструктури. Хоча такі функції здійснювалися і раніше Службою безпеки України, але їх виконання на пов'язувалося з категорією «критична інфраструктура».

В Стратегії кібербезпеки України термін «критична інформаційна інфраструктура» отримав таке тлумачення (в «1. Загальні положення»): «інформаційної інфраструктури, яка знаходиться під юрисдикцією України та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України». По тексту цього документу неодноразово використовується термін «критична інфраструктура» в поєднанні з поняттями «об'єкт», «кіберзахист» і т.д., що знову ж таки створює проблему прив'язки

[25] COM (2009)149: Communication from the Commission on Critical Information Infrastructure Protection: Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. – Brussels, 2009 - link

функцій захисту до певної категорії об'єктів, яка нормативно не визначена. Взагалі треба відмітити, що нормативні та організаційні основи забезпечення кібер-безпеки розвиваються паралельно із захистом критичної інфраструктури, про свідчать офіційні документи Європейської Комісії [25].

Слід також сказати, що додатковим стимулом для впровадження захисту критичної інфраструктури в Україні є необхідність гармонізації вітчизняного законодавства та підходів до забезпечення національної безпеки з тими, що є визнаними у країнах-членах ЄС та НАТО. Тому, як позитивний момент слід відмітити те, що в Річній національній програмі співробітництва Україна-НАТО на 2016 рік міститься окремий пункт 1.3.2 «Захист критичної інфраструктури», в якому названі пріоритети забезпечення захисту критичної інфраструктури, які фактично повторюють положення Стратегії національної безпеки та стратегічні цілі державної політики в цьому напрямі, зазначені в Зеленій книзі.

Висновок

Зважаючи на неспокійну безпекову ситуацію навколо України, євроатлантичні поступи нашої держави, реформування сектору безпеки і оборони, вже усвідомлено необхідність створення повноцінної системи захисту критичної інфраструктури. Нині можна говорити про поступове проникнення елементів цього підходу в нормативні документи, і відповідно в практику виконання без пековими відомствами своїх функцій.

Вкрай важливим є той момент, що захист критичної інфраструктури здійснюється в умовах де-юре мирного часу, а де-факто – ведення гібридної війни проти Української держави. Враховуючи це, можна говорити про захист критичної інфраструктури як новий компонент безпекової політики, що спрямовані на забезпечення сталого функціонування суспільства, економіки та державного управління в умовах сучасних викликів.

Список учасників

№	П І Б	Організація, посада
1	БІРЮКОВ Дмитро Сергійович	Національний інститут стратегічних досліджень, Завідувач сектору техногенної безпеки
2	БОБРО Дмитро Геннадійович	Національний інститут стратегічних досліджень, Провідний науковий співробітник
3	БОГДАНОВИЧ Володимир Юрійович	Міністерство оборони, Головний науковий співробітник ЦНДІ ЗС України
4	БОЙЧУН Олег Володимирович	Координаційна рада Платформи з енергетичної безпеки, Голова
5	БУГАР Олег Вікторович	ДП «Укравтогаз», Заступник головного інженера
6	ВИШНЕВСЬКА-ЧЕРКАС Ірина Григорівна	Міністерство закордонних справ, Третій секретар відділу НАТО Департаменту міжнародної безпеки МЗС України;
7	ВДОВЕНКО Віталій Григорович	Верховна Рада України, Комітет з питань паливно-енергетичного комплексу, ядерної політики та ядерної безпеки, Головний консультант секретаріату
8	ВЛАСЮК Олександр Степанович	Національний інститут стратегічних досліджень, Перший заступник директора
9	ГИЧКА Олег	Центр «Стратегія XXI», Експерт
10	ГОЛІКОВА Світлана Веніамінівна	Компанія «ТрансЕнергоКонсалтинг», Директор
11	ГОНЧАР Михайло Михайлович	Центр глобалістики «Стратегія XXI», Президент
12	ГОНЧАР Христина Михайлівна	Київський міжнародний енергетичний Q-клуб, Виконавчий директор
13	ГУНДА Микола Васильович	ДП «Науканафтогаз», Заступник директора
14	ДЯЧЕНКО Сергій Миколайович	Бюро комплексного аналізу та прогнозів, Голова Бюро
15	ЄВДІН Олександр Миколайович	ДСНС, Український науково-дослідний інститут цивільного захисту, Перший заступник начальника
16	КНЯЖАНСЬКИЙ Віталій	Газета «День»
17	КОЧЕРГА Данило Анатолійович	Національна гвардія України, Начальник служби стратегічного планування відділу стратегічного планування та сумісництва з ВС НАТО оперативного управління штабу ГУ
18	КУДІН Сергій Анатолійович	Державна служба з надзвичайних ситуацій, Заступник начальника відділу оперативно-чергової служби та готовності пунктів управління Департаменту реагування на надзвичайні ситуації
19	КУНИЦЬКИЙ Ігор Миколайович	ДП «НАЕК «Енергоатом», Начальник відділу протидії актам ЯТ, СП та ООЖ Дирекції фізичного захисту та спеціальної перевірки

№	П І Б	Організація, посада
20	ЛАКІЙЧУК Павло	Центр «Стратегія ХХІ», Експерт
21	ЛІСОВСЬКИЙ Валерій Францович	НАК «Нафтогаз України», Заступник начальника управління Департаменту економічної, промислової, інформаційної безпеки та управління ризиками
22	МАНДРАГЕЛЯ Володимир	Національна академія державного управління при Президентові України, Професор
23	МАРТИНЕНКО Сергій Васильович	Міністерство оборони України, Старший офіцер електротехнічної служби Збройних Сил України
24	МЕДВІДЬ Валентин Олександрович	ПАТ «Укртранснафта», Директор з охоронної діяльності та економічної безпеки
25	МОРОЗ Оксана В'ячеславівна	Міністерство енергетики та вугільної промисловості України, Головний спеціаліст Управління стратегії розвитку паливно-енергетичного комплексу та інвестиційної політики
26	НАГОРНИЙ Сергій Сергійович	ГО «Українська конфедерація журналістів», Генеральний директор міжнародного проекту
27	НЕДРЯ Максим	Центр «Стратегія ХХІ», Експерт
28	НЕСТЕРЕНКО В'ячеслав Миколайович	Міністерство оборони України, Начальник відділу енергозбереження управління експлуатації Головного квартирно-експлуатаційного управління ЗС України
29	ОМЕЛЬЧЕНКО Володимир Юрійович	Центр Разумкова, Директор енергетичних програм
30	ПІНЧУК Михайло Георгійович	ПАТ «Укргідроенерго», Директор департаменту фізичного захисту, режиму та безпеки
31	ПОЛТОРАЦЬКИЙ Олег Володимирович	ДП «НАЕК «Енергоатом», Начальник сектору з протидії актам ЯТ, СП та ООЖ Дирекції фізичного захисту та спеціальної перевірки
32	ПОНОМАРЕНКО Ігор Олексійович	Київський міжнародний енергетичний Q-клуб, Керівник напрямку «Газовий транспорт»
33	ПОПЛАВСЬКА Оксана Володимирівна	Міненерговугілля, головний спеціаліст відділу двостороннього та багатостороннього співробітництва Департаменту стратегічного планування та європейської інтеграції
34	ПОПОВИЧ Владислав Іванович	Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг, Начальник управління інформаційних технологій
35	РОМАНОВСЬКИЙ Владислав Васильович	Національна гвардія України, Заступник начальника оперативного управління штабу Головного управління
36	СИНИЦЯ Світлана Леонідівна	Київський міжнародний енергетичний Q-клуб, Менеджер проектів
37	СКРИПІН Ігор Олександрович	Служба безпеки України Начальник відділу

№	П І Б	Організація, посада
38	СОКОЛОВ Сергій Володимирович	КНЕУ ім.В.Гетьмана
39	СУХОДОЛЯ Олександр Михайлович	Національний інститут стратегічних досліджень, Завідувач відділу енергетичної та техногенної безпеки
40	УГОЛЬКОВ Ігор Валерійович	Національна гвардія України, Начальник відділу фізичного захисту ЯУ управління з охорони важливих державних об'єктів штабу ГУ
41	ХОМІЧ Михайло Сергійович	Національна поліція України, Інспектор департаменту кіберполіції
42	ЧОРНОГОР Ярослав	ДУ «Інститут всесвітньої історії НАН України», С.н.с. відділу трансатлантичних досліджень
43	ЧУБИК Андрій Олександрович	Центр «Стратегія ХХІ», Виконавчий директор
44	ЧУМАЧЕНКО Сергій Миколайович	ДСНС, Український науково-дослідний інститут цивільного захисту, Начальник відділу моделювання надзвичайних ситуацій Науково-дослідного центру інноваційних технологій
45	ШТЕЛЮК Сергій Миколайович	Міністерство закордонних справ, Начальник відділу міжнародного галузевого та інвестиційного співробітництва Управління економічного співробітництва МЗС України
Іноземні учасники		
46	БАГДОНАС Гінтарас (Gintaras BAGDONAS)	Центр передового досвіду НАТО з питань енергетичної безпеки, Директор (Литва)
47	ГАЄК Ярослав (Jaroslav HAJEK)	Центр передового досвіду НАТО з питань енергетичної безпеки, Експерт (Чехія)
48	ГЛУШКЕ Гідо (Guido GLUSCHKE)	Бранденбурзький університет прикладних наук, Співдиректор Інституту з проблем безпеки (Німеччина)
49	ЕНКЕ Флоріан (Encke Florian)	Штаб-квартира НАТО, Департамент з політичних питань і політики безпеки (Бельгія)
50	ЛОСКОТ-СТРАХОТА Агата (Loskot-Strachota Agata)	Центр східних досліджень (Польща)
51	ТОМАШЕК Якуб (Tomasek Jakub)	Празький інститут безпекових студій (Чехія)
52	ШОРТ Бенджамін (Benjamin SHORT)	Центр передового досвіду НАТО з питань енергетичної безпеки, Експерт
53	КОСТ Павел (KOST Pawel)	Центр дослідження армії, конверсії та роззброєння (Польща)
54	ЛЕСК Геррі (LESK Gerri)	Посольство Естонії в Україні (Естонія)
55	ХМЕЛАРОВА Альжбета (CHMELAROVA Alzbeta)	Посольство Чеської Республіки в Україні (Чехія)
56	KALINOWSKI Jan КАЛІНОВСЬКИ Ян	Посольство Республіки Польща в Україні (Польща)

Невоєнний вимір війн нового покоління. Енергетичний компонент
Матеріали за підсумками міжнародної конференції

Упорядники:
Бобро Д.Г., провідний науковий співробітник відділу енергетичної та техногенної безпеки НІСД, к. ф.-м. н.
Синиця С. Л., керівник проекту Київського міжнародного енергетичного клубу
Під загальною редакцією Гончара М. М., президента Центру глобалістики «Стратегія XXI»; Суходолі О. М., доктора наук з державного управління, професора, завідувача відділу енергетичної та техногенної безпеки НІСД

Електронна версія: http://niss.gov.ua http://geostrategy.org.ua http://qclub.org.ua

За підтримки: