Co-funded by the
Erasmus+ Programme
of the European Union

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФРАСТРУКТУРИ ТА ТЕХНОЛОГІЙ

ФАКУЛЬТЕТ УПРАВЛІННЯ І ТЕХНОЛОГІЙ
КАФЕДРА МЕНЕДЖМЕНТУ, ПУБЛІЧНОГО УПРАВЛІННЯ ТА
АДМІНІСТРУВАННЯ

ГІБРИДНІ ЗАГРОЗИ ТА КОМПЛЕКСНА БЕЗПЕКА

Навчальний посібник
для здобувачів другого (магістерського)
рівня вищої освіти

Київ – 2024

Co-funded by the Erasmus+ Programme of the European Union

УДК 351.861
Г46

Рекомендовано до друку Вченою радою
Державного університету інфраструктури та технологій
Міністерства освіти і науки України*(протокол №12 від 28 червня 2024р.)*

РЕЦЕНЗЕНТИ:

Худолей В.Ю., доктор економічних наук, професор, ректор Закладу вищої освіти «Міжнародний науково-технічний університет імені академіка Юрія Бугая»;

Ложачевська О.М,, доктор економічних наук, професор, завідувач кафедри менеджменту Національного транспортного університету Міністерства освіти і науки України;

Паливода О.М., доктор економічних наук, професор, професор кафедри менеджменту зовнішньоекономічної діяльності підприємства Національного авіаційного університету Міністерства освіти і науки України.

Г46 Гібридні загрози та комплексна безпека: навчальний посібник. Укл. Карпенко О.О., Осипова Є.Л. Київ : ТОВ «ТРОПЕА», 2024. 76 с.
DOI: https://doi.org/10.32703/978-617-8268-30-5
ISBN 978-617-8268-30-5

У навчальному посібнику досліджено еволюції гібридних загроз та їхній можливий подальший розвиток. Проаналізовано сучасні тенденції стратегічного розвитку підприємств. Визначено загальнотеоретичні засади гібридних загроз. Значну роль відведено ознайомленню з концепцією гібридних загроз. Представлений навчальний посібник буде корисним для формування системи знань та вмінь, необхідних для виконання організаційних, аналітичних та консультаційних функцій щодо ідентифікації та протидії гібридним загрозам і забезпечення комплексної безпеки на національному й міжнародному рівні..

Навчальний посібник підготовлено на основі матеріалів проєкту WARN «Академічна протидія гібридним загрозам» (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP), що співфінансується програмою Erasmus+ Європейського Союзу. Підтримка Європейською Комісією у створення матеріалів, розміщених у даному навчальному посібнику, не є схваленням змісту, який відображає погляди лише авторів, і Комісія не несе відповідальності за будь-яке використання інформації, що міститься у ньому.

Рекомендується для здобувачів та викладачів закладів вищої освіти, наукових співробітників, спеціалістів підприємств, органів державного управління та всіх зацікавлених осіб.

ISBN 978-617-8268-30-5 УДК 351.861

ЗМІСТ

ПЕРЕДМОВА

Однією з відповідей на численні виклики, які зумовлені впливом гібридних загроз, є реалізація проєкту «Академічна протидія гібридним загрозам» (WARN) в межах Програми ЄС Еразмус+ за напрямом «Розвиток потенціалу вищої освіти» (Erasmus+ Capacity Building Project 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP). Вебсайт проєкту WARN: http://warn-erasmus.eu.

Місія проєкту – підвищення національної безпеки та подолання нестачі сервісів безпеки, яка виникла через появу гібридних загроз. Цільові групи: студенти, університети, викладачі, компанії та організації, суспільство загалом.

Над виконанням проєкту працюють європейські та українські університети:

- Університет Ювяскюля, Фінляндія - власник грантів та координатор;
- ECAM-EPMI (Вища інженерна школа), Франція;
- Університет Коїмбри, Португалія;
- Університет Тарту, Естонія;
- Харківський національний університет радіоелектроніки, Україна;
- Український католицький університет, Україна;
- Державний університет інфраструктури та технологій, Україна;
- Національний університет «Острозька Академія», Україна;
- Національна академія керівних кадрів культури і мистецтв, Україна;
- Харківський регіональний інститут державного управління Харківського національного університету ім. В. Н. Каразіна, Україна;
- Горлівський інститут іноземних мов ДВНЗ «Донбаський державний педагогічний університет», Україна.

Разом виконавці проєкту працюють над розбудовою безпечного громадянського середовища в Україні.

За результатами реалізації проєкту:

1) замість оновлення одинадцяти заявлених магістерських освітніх програм, парнери проєкту оновли дванадцять програм («Публічне управління та адміністрування»; «Управління фінансово-економічною безпекою»; «Системи штучного інтелекту»; «Менеджмент організацій і адміністрування»; «Інженерія програмного забезпечення»; «Менеджмент соціокультурної діяльності»; «Середня освіта (історія)»; «Національна безпека»; «Політологія»; «Медіакомунікації»; «Економіка»; «Журналістика») та створили абсолютно нову магістерську програму («Публічна політика і управління в умовах гібридних загроз») завдяки додаванню курсів, сфокусованих на протидію гібридним загрозам відповідно до останніх рекомендацій та практики партнерів з ЄС;

2) розроблено 12 нових курсів (один загальний курс: «Гібридні загрози та комплексна безпека» та 11 спеціальних курсів щодо розпізнавання та протидії гібридним загрозам у певних областях) та оновлено 39 курсів;

3) створено та обладнано 7 центрів передового досвіду (на базі оновлених лабораторій);

4) розроблено один електронний посібник за новою методикою гібридного навчання «Методика навчання в умовах гібридних загроз» (єдиний для всіх партнерів);

6) запроваджено викладання адаптованих освітніх програм і курсів;

7) навчання пройшли 493 студенти за оновленими освітніми програмами (за 2022-2023 навчальний рік);

8) підвищення кваліфікації пройшли 2018 слухачів LLL-курсів для безперервного професійного розвитку (за 2022-2023 навчальний рік);

9) опубліковано статті в журналах, тези на конференціях, публікації на професійних та освітніх веб-сайтах;

10) проведено спільні заходи за інформацією з офіційних інституційних, національних та міжнародних баз даних та інформаційних сторінок, зокрема чотири конференції «Управління та адміністрування в умовах протидії гібридним загрозам національній безпеці» (у 2020, 2021, 2022 та 2023 роках);

11) триває процес створення міжгалузевого середовища з питань протидії гібридним загрозам, зокрема у жовтні 2022 року Заклад вищої освіти «Міжнародний науково-технічний університет імені академіка Юрія Бугая» приєднався до WARN-середовища.

Участь у проєкті WARN показала, що одним з ефективних напрямків розвитку в країні системи протидії гібридним загрозам є освіта. Заклади вищої освіти України шляхом впровадження відповідних навчальних дисциплін та організації курсів підвищення кваліфікації здійснюють роз'яснення сутності, інформування про гібридні загрози, можливості та способи їх попередження, а також мінімізації негативних наслідків впливу гібридних загроз.

Отже, для того, щоб протидіяти гібридним загрозам потрібно використовувати різноманітні методи для підвищення освіченості у різних професійних сферах, розвитку критичного мислення та медіаграмотності, забезпечення інформаційної стійкості, а також співпрацювати з різними групами в суспільстві, налагодити комунікацію між громадськістю та владою. Все це в комплексі дозволить забезпечити національну стійкість, суверенність нашої держави і зберегти національну ідентичність.

РОЗДІЛ 1.
АСИМЕТРІЯ, ГІБРИДНІ ЗАГРОЗИ ТА БЕЗПЕКА

1.1. Предмет і завдання курсу
1.2. Новий безпековий ландшафт та прийняття рішень
1.3. Гібридні загрози - історія, визначення, основні характеристики
1.4. Спектр PMESII; «4+1+AI» (land, air, sea, space + cyber+ AI)

1.1. Предмет і завдання курсу

Мета вивчення дисципліни «Гібридні загрози та комплексна безпека» - формування системи знань та вмінь, необхідних для виконання організаційних, аналітичних та консультаційних функцій щодо ідентифікації та протидії гібридним загрозам і забезпечення комплексної безпеки на національному й міжнародному рівні.

Курс розроблено та впроваджено з метою виконання завдань міжнародного проєкту Erasmus + «Академічна протидія гібридним загрозам» (Academic Response to Hybrid Threat, WARN), який реалізується в межах Програми Європейського Союзу Еразмус+ за напрямом «Розвиток потенціалу вищої освіти» (Erasmus+ Capacity Building Project 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP). Вебсайт проєкту WARN: http://warn-erasmus.eu.

Завдання вивчення дисципліни «Гібридні загрози та комплексна безпека»:

- вивчення загальнотеоретичних засад гібридних загроз
- вивчення еволюції гібридних загроз та їхній можливий подальший розвиток;
- формування у здобувачів знань про понятійно-категоріальний апарат теорії гібридних загроз;
- ознайомлення з концепцією гібридних загроз;
- вивчення сучасних доменів (сфер) та інструментів гібридних загроз;
- формування критичного мислення, навичок розпізнавання гібридних загроз;
- формування вмінь і навичок протидії гібридним загрозам і забезпечення комплексної безпеки.

У результаті вивчення дисципліни «Гібридні загрози та комплексна безпека» здобувачі повинні:

знати загальнотеоретичні засади гібридних загроз, понятійно-категоріальний апарат теорії гібридних загроз і комплексної безпеки; вимоги протидії гібридним загрозам і забезпечення комплексної безпеки; сучасні домени (сфери) та інструменти гібридних загроз; закономірності гібридних загроз і комплексної безпеки на тлі світової політики та політики окремих країн та регіонів.

вміти:

- застосовувати критичне мислення, раціональну аргументацію, аналіз та синтез.
- постійно вчитися та оволодівати сучасними професійними знаннями.
- проводити професійний пошук, оброблення та аналіз фактів, даних та інформації з різних первинних та вторинних джерел.
- застосовувати відповідні поняття, теорії і методи до аналізу гібридних загроз і комплексної безпеки стосовно політичних акторів, інститутів та ідей відповідно до певного історичного або сучасного контексту.
- використовувати сучасні теорії гібридних загроз, концепти та методи комплексної безпеки для інтерпретації та змістовного аналізу гібридних загроз і комплексної безпеки на місцевому, національному та міжнародному рівні.

1.2. Новий безпековий ландшафт та прийняття рішень

У сучасному глобалізованому світі проблема забезпечення стійкості держави і суспільства до загроз різного характеру стає все більш актуальною, особливо, коли ці загрози трансформуються і набувають нових гібридних форм. Так, за умов швидкого розвитку інформаційних технологій нині вже не обов'язково вдаватися до відкритої збройної агресії для нанесення відчутних втрат супротивнику. Іноді достатньо вивести з ладу (тимчасово чи на більш тривалий час) деякі об'єкти критичної інфраструктури або ключові соціальні, економічні чи військові ресурси держави [1].

Глобальне безпекове середовище характеризується високим рівнем турбулентності й непередбачуваності, руйнується міжнародна система стратегічної стабільності, загострюється конкуренція між державами, виникають нові конфлікти, урегулювати які стає все складніше [2].

Прийняття рішень базується на певних системах цінностей, які виконують роль внутрішнього арбітра. Система цінностей містить набір параметрів та критеріїв (правил), за якими відбувається прийняття рішень. Новий безпековий ландшафт сприяє розмиванню системи цінностей, граючи на межі понять. Якщо стерти чітку грань між категоріями (війна-мир, добре-погано, друг-ворог тощо), то виникає «сіра зона» невизначеності, в якій прийняття рішень буде нестійким, потенційно вразливим. Гібридні гравці намагаються не переконати, не битись, а вплинути на алгоритм прийняття рішень [3].

Науковці виділяють три підходи до сутності поняття «управлінське рішення» [4]. У рамках першого підходу управлінське рішення розглядається як процес, тобто сукупність низки послідовних дій, спрямованих на вирішення конкретної ситуації. Другий підхід полягає в тому, що управлінське рішення можна трактувати як акт вибору особою, що приймає його за допомогою

визначених правил. Відповідно до третього підходу управлінське рішення описується як результат вибору.

Загалом управлінські рішення повинні відповідати деяким вимогам [5]: бути своєчасними, ефективними, економічними, чітко сформованими й обґрунтованими.

Управлінські рішення завжди спрямовані на розв'язання конкретних управлінських завдань, які характеризуються: невизначеністю, а в деяких випадках і суперечливістю умов; недостатністю інформації про можливі способи їх вирішення та чітких алгоритмів вирішення; необхідністю вирішення в обмежений час [6].

Ключову роль у процесі прийняття рішень займає особа (група осіб), яка приймає рішення. Для формування механізму прийняття рішень у новому безпековому ландшафті особі (групі осіб), яка приймає рішення, необхідно [3]:

- підвищувати освіченість у різних сферах, оскільки прийняття рішень вимагає системного підходу. Особи, які приймають рішення, мають оцінювати всі окремі загрози та ризики як елементи єдиної «картини», а не аналізувати їх окремо;
- розвивати критичне мислення, оскільки вміння розрізняти джерела та призначення інформації, обмірковувати, аналізувати та ставити питання дозволяє уникнути впливу маніпуляцій та окремих агентів, що поширюють неправдиву інформацію;
- забезпечувати когнітивну стійкість, оскільки у новому безпековому ландшафті людська свідомість стає полем бою. Мета когнітивної війни полягає в зміненні не лише того, що думає людина, а й того, як вона думає і діє [7]. Когнітивна війна прагне посіяти сумніви, запровадити суперечливі наративи, поляризувати громадську думку, радикалізувати групи і спонукати їх до дій, які можуть зруйнувати або розділити згуртоване суспільство;
- посилювати інформаційну стійкість, що формує вміння перевіряти та знаходити достовірну надійну актуальну інформацію.

1.3. Гібридні загрози - історія, визначення, основні характеристики

У сучасних умовах війна істотним чином змінила свою сутність та зміст, отримавши гібридний характер, хоча, як вважають експерти, такі ознаки війни не є абсолютно новітніми і безпрецедентними. Іншими словами, гібридні війни не є чимось новим у світовій історії. Гібридні війни використовувались у різних формах і з різними масштабами протягом багатьох десятиліть і навіть століть. Тому, хоча форми та методи гібридних війн можуть змінюватися, історичний контекст і механізми міждержавних конфліктів можуть залишатися подібними [8].

Так, ще видатний китайський стратег і мислитель Сунь-Цзи, що жив в VI-V ст. до н.е., у своєму відомому трактаті про військову стратегію «Мистецтво війни» наголошував: «Здобути сто перемог у ста битвах – це не вершина військового мистецтва. Повалити ворога без бою – ось вершина». Якщо як основний інструмент вирішення міждержавних протиріч та протистояння обирається військова сфера – застосування збройних сил – виникає війна в її класичному розумінні. Якщо досягнення мети агресії здійснюється шляхом комплексних заходів у політичній, економічній та інформаційній сферах, а воєнні дії мають обмежений, допоміжний характер – виникає соціально-політичне явище, яке отримало назву гібридної війни. У ході гібридної війни агресія ведеться в усіх чотирьох сферах – політичній, економічній, інформаційній та воєнній – одночасно. Отже, на перший план виходить не силова, а інформаційна, суспільна-політична, ідеологічна та економічна складові впливу на супротивника [9].

Наприкінці XX – початку XXI століття відбулося переосмислення концепту «війни» у працях західних дослідників (табл 1.1).

Гібридна війна – це синхронізоване використання багатьох інструментів впливу, підібраних з урахуванням конкретних вразливостей в усьому спектрі соціальних функцій для досягнення синергетичних ефектів [14].

Таблиця 1.1

Характеристика концепту «війни»

Автор, джерело	Характеристика концепту «війни»
Kaldor M. [10]	виокремлює два типи війни – «старі війни» та «нові війни». Перші представляють нам концепт Карла фон Клаузевіца, де війна – це типові міждержавні війни XIX–XX століття, що базуються на політичному протистоянні засобами озброєння, вертикальною структурою та вирішальними битвами. «Нові», або сучасні війни, на думку М. Кальдор, подібні до соціального стану або навіть спільного підприємства, ніж до змагань. Вони охоплюють багатоманітні збройні формування, що досягають своєї цілі та отримують прибуток від насилля самого по собі, а не від перемоги чи поразки.
Hoffman F., Mattis James N. [11]	аналізуючи сучасні війни, варто звернути увагу на процес технологічного вдосконалення та зростання нетрадиційних методів ведення війни. Цей «безпрецедентний синтез» різних комбінацій технологій, тактик, засобів, де одну з домінуючих ролей відіграватимуть недержавні іррегулярні формування, дослідники називають гібридними війнами.
Schmid Johann [12]	аналізує особливості гібридних війн, порівнюючи ієрархічну та неієрархічну моделі війни з точки зору центру удару та виокремлює три особливості гібридних війн: (1) Основна мета – вплив на вирішення конфлікту невійськовими засобами, тобто спрямованість на досягнення успіху в психологічному, моральному та правовому середовищі, а не у військовому тиску. (2) Латентне та багаторівневе поєднання різних типів, форм та концепцій війни та ведення бойових дій. Латентна форма полягає у асиметричному впливі та маніпулюванні механізмами прийняття рішень завдяки контролю семантичного поля або габітусу суспільства, тобто формується необхідна когнітивна платформа у об'єктів впливу. (3) Розмиття встановлених категорій порядку шляхом навмисного функціонування *у сірих зонах* різних інтерфейсів, тобто шляхом впливу на аксіологічний стан суспільства та його політичну культуру відбувається трансформація громадських настроїв та дискредитація демократичної системи прийняття рішень та цінностей

Джерело: складено на основі [10-13]

Термін «гібридні загрози» походить від поняття, що з'явилося раніше – «гібридні війни», адже саме гібридні загрози стали серйозним викликом у сучасному світі для багатьох країн, включаючи Україну. Вони поєднують у собі різні методи, такі як інформаційна війна, кібератаки, економічний тиск, дезінформація та інші форми неконвенційних дій, що реалізуються з метою підриву стійкості, національної єдності та суверенітету країни, що стає мішенню гібридних загроз. Понятійний апарат гібридних загроз детально проаналізовано у Глосарії з гібридних загроз [15], що є одним з вагомих результатів реалізації проєкту WARN [16] (табл. 1.2).

Таблиця 1.2

Характеристика поняття «гібридні загрози»

Джерело	Визначення поняття «гібридні загрози»
Hybrid CoE [17]	Скоординовані та синхронізовані дії, які навмисно спрямовані на системні вразливості демократичних держав та інститутів, за використанням широкого кола засобів; діяльність, яка використовує пороги виявлення та атрибуції, а також різні інтерфейси (війна-мир, внутрішня-зовнішня безпека, локальний-державний та національний-міжнародний); діяльність, спрямована на вплив на різні форми прийняття рішень на місцевому (регіональному), державному або інституційному рівнях і покликана сприяти та/або досягати стратегічних цілей агента, підриваючи та/або завдаючи шкоди об'єкту.
Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K., & McCue, M. (2018) [18]	"…загрози, створені супротивниками, з можливістю одночасно адаптивно застосовувати звичайні та нетрадиційні засоби для досягнення своїх цілей."
Pawlak P. (2017) [19]	Явище, що виникає в результаті конвергенції та поєднання різних елементів, які разом утворюють більш складну та багатовимірну загрозу (на відміну від Гібридного Конфлікту, Гібридної війни).
Horbulin Volodymyr (2017) [20]	Соціально небезпечні події, явища або процеси, породжені змінами у глобальному безпековому довкіллі в результаті синергії, утвореної від використання агресором і) звичайних збройних сил та можливостей та ii) нетрадиційних форм ведення війни (тероризм, злочинна діяльність, "громадянська війна", диверсія тощо), а також iii) невійськові способи впливу, які трансформувались у зброю в різних сферах операцій (дипломатичних, інформаційних, економічних, фінансових, торгових, соціальних тощо). Мають на меті примусити об'єкт агресії до вимог, що суперечать його національним інтересам, незалежно від оголошення війни. Одним із можливих способів здійснення гібридних загроз є організація та підтримка сепаратистських рухів, які можуть порушити суверенітет та територіальну цілісність об'єкта агресії.
Joint Framework on countering hybrid threats the European Union response (2016) [21]	Концепт, спрямований на охоплення комбінації силових та підривних традиційних та нетрадиційних методів (наприклад, дипломатичні, військові, економічні, технологічні), які можуть використовуватися скоординовано державними та недержавними акторами для досягнення певних цілей поза офіційним оголошенням війни.
Sadık Giray (2017) [22]	Загальний термін, що охоплює широкий спектр наявних негативних явищ та тенденцій (тероризм, міграція, піратство, корупція, етнічні конфлікти тощо), які адаптативно та системно використовуються для досягнення політичних цілей. При цьому суб'єктами таких загроз виступають недержавні та державні актори.
Wigell Mikael (2019) [23]	Визначає цілі гібридних загроз: деструктивізм суспільства та синхронізований вплив на нього, тобто використання комплексу різних засобів для створення розділення (роздробленості) у суспільстві; стратегія латентного маніпулювання іншими державними стратегічними інтересами; вплив актора на механізм прийняття рішень з метою отримання бажаного результату (рішення).

Джерело: складено на основі [13; 15; 17-23]

Поняття «гібридні загрози» відноситься до дій, які здійснюються державними чи недержавними акторами, мета яких полягає в тому, щоб підірвати або завдати шкоди цільовій групі шляхом здійснення впливу на її прийняття рішень на місцевому, регіональному, державному чи інституційному рівні. Такі дії координуються і синхронізуються та навмисно націлені на вразливі місця демократичних держав та інститутів. Дії можуть мати місце, наприклад, у політичній, економічній, військовій, громадянській або інформаційній сферах. Вони проводяться з використанням широкого кола засобів і розраховані на те, щоб залишатися нижче порога виявлення і атрибуції [17].

Таким чином, поняття «гібридні загрози» та «гібридні війни» є спорідненими. Основними спільними рисами є діяльність державних та недержавних ворожих акторів різних рівнів; асиметричний характер впливу, тобто нелінійні, багаторівневі та латентні атаки на різноманітні сфери життєдіяльності суспільства; комбінування традиційного та нетрадиційного інструментарію впливу, при цьому спостерігається домінування невійськових засобів досягнення стратегічних та тактичних цілей.

Погоджуючись з висновком Реви Т. [13], слід відзначити, що поняття «гібридні загрози» є ширшим за поняття «гібридні війни», тобто охоплює різноманітні явища, що несуть деструктивний характер для демократичного режиму завдяки застосуванню комбінацій різних методів, де гібридні війни виступають одним з найефективніших засобів впливу.

1.4. Спектр PMESII; «4+1+AI» (land, air, sea, space + cyber+ AI)

На цей час для аналізу комплексної стратегічної та оперативної обстановки НАТО використовує конструкцію PMESII (Politics, Military, Economy, Society, Information Structure, Infrastructure), що має шість основних доменів [24]:

P – Політичний. Будь-яке об'єднання цивільних акторів, організацій та установ, як офіційних, так і неформальних, що мають владу / керують в певних географічних межах або організацій і застосовують різні форми, інструменти політичної влади та впливу. Сюди включаються політична система, партії та основні актори, а також культурні, історичні, демографічні, релігійні фактори, що формують ідентичність суспільства.

M – Військовий. Збройні сили та допоміжна інфраструктура, що створені, підготовлені, розвиваються і підтримуються для досягнення та захисту національних або організаційних цілей безпеки. Сюди включаються також аспекти внутрішньої безпеки країни.

E – Економічний. Складається із загального обсягу виробництва, розподілу та споживання всіх товарів і послуг для країни чи організації. Сюди включається не тільки економічний розвиток країни, але й розподіл багатства.

S – Соціальний. Взаємозалежна мережа соціальних інститутів, які підтримують, надають різні можливості, культурно об'єднують окремих осіб та

забезпечують участь у досягненні особистих і життєвих цілей у межах спадкових та неспадкових груп як у стабільному, так і в нестабільному середовищі. Домен охоплює такі соціальні аспекти, як релігія, структура суспільства, правова та судова система, поліція, гуманітарна діяльність.

І – Інфраструктура. Основні об'єкти, послуги та обладнання, необхідні для функціонування громади, організації чи суспільства. Включає логістичну, комунікаційну і транспортну інфраструктуру, школи, лікарні, розподіл води та електроенергії, каналізацію, зрошення, географічне положення тощо.

І – Інформація. Вся інфраструктура, організація, персонал і компоненти, які збирають, обробляють, зберігають, передають, відображають, поширюють та використовують інформацію. Охоплює інформацію та медіакомунікації.

Пізніше до спектру було додано дві додаткові змінні - фізичне середовище (Physical Environment - P) та час (Time - T). Зважаючи на військову значимість цих чинників, автори проілюстрували зв'язок між часом, топографічними, кліматичними і екологічними особливостями, пов'язаними з проведенням військових операції. Однак, окрім військових наслідків, можна помітити економічні, а також інфраструктурні кореляції. Природні ресурси країни та її загальна здатність розподіляти ці ресурси можуть суттєво впливати на операційне середовище [25].

Збір інформації здійснюється з метою розуміння цивільного середовища, процесів, які в ньому відбуваються, та яким чином зазначене може вплинути на ефективність виконання завдань військами (силами) (рис. 1.1).

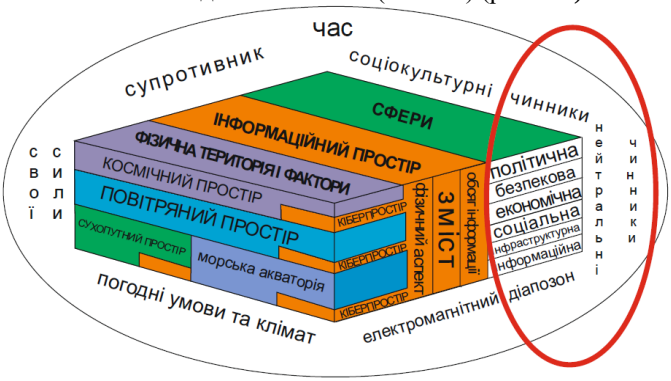

Рис.1.1. Єдиний погляд на умови оперативної обстановки
Джерело: [26]

Розуміння цивільного середовища досягається шляхом застосування процедур оцінювання цивільного середовища. Результатом завершення цього етапу є підготовка документа – оцінки цивільного середовища.

Згідно з військовими стандартами НАТО існує два етапи (види) оцінки

цивільного середовища (ОЦС):

1 – встановлення (визначення) ключових осіб цивільного середовища, попередня оцінка об'єктів цивільного середовища (англ. – "CIMIC estimate");

2 – безпосередньо ОЦС (з висновками) як складова загальної оцінки оперативної обстановки (англ. – "operations assessment").

У висновках з ОЦС деталізується, які саме чинники в різних сферах оцінки мають або можуть мати найбільший вплив у районі виконання завдань військами і сприятимуть або перешкоджатимуть цьому (рис. 1.2).

Рис.1.2. Вплив чинників макросередовища на об'єкт аналізу
Джерело: [26]

Висновки з оцінки цивільного середовища за методом PMESII-PT-аналізу робляться в короткому вигляді за кожним з аспектів. При цьому мають бути проаналізовані:

- політичні аспекти – ключові елементи формального, неформального та тіньового управління і яке вони мають відношення до цивільного населення і загальної стабільності;
- військові аспекти – основні елементи, що впливають на ситуацію в сфері безпеки і стабільності;
- економічні аспекти – ключові елементи економічної стабільності та активності;
- соціальні аспекти – ключові елементи, що впливають на традиційну соціальну динаміку;
- інфраструктурні аспекти – основні засоби, послуги, що впливають на загальну стабільність та їх значимість для населення;
- інформаційні аспекти – ключові елементи та основні засоби, що впливають на інформаційний простір.

Загальний висновок повинен дати відповідь на запитання: чи сприяє

ситуація в цивільному середовищі виконанню завдань? Якщо ні – то які чинники матимуть найбільший (вирішальний) вплив на їх виконання.

Технології на основі штучного інтелекту (AI) активно використовуються в усіх сферах. З плином часу та зі зменшенням складності реалізації рішень на основі AI, у світі почали з'являтися випадки використання технологій на основі штучного інтелекту в військових цілях. У зв'язку із швидкими темпами розвитку технологій AI – світ перейшов на етап гонки озброєнь зі штучним інтелектом. Гонка озброєнь AI в розпалі між такими країнами, як Китай, росія і США. Наслідки застосування зброї, а також її використання в рамках кібербезпеки та її захист від різних загроз повинні викликати першочергове занепокоєння. Оскільки AI розробляється в основному приватними компаніями, існує брак адекватного регулювання з боку держави, проте деякі країни, такі як Канада, Китай, Індія, Об'єднані Арабські Емірати, Сполучене Королівство та США, зробили нові кроки в цьому напрямку [27].

У стратегічних дослідженнях робота над AI не береться до уваги, зокрема у військових стратегіях і плануванні [28]. Використання AI в стратегічних дослідженнях може революціонізувати військові операції, а також принести користь міжнародній безпеці завдяки кращим і ефективнішим рішенням для прийняття рішень. Дослідники прогнозують, що проміжний варіант допоможе військовим операціям і це буде еволюційним кроком в аспекті прийняття рішень за допомогою штучного інтелекту. Вони досліджували наступні чотири аспекти [28]:

- сам AI, що швидко розвивається;
- використання AI в кіберпросторі і кібербезпеці;
- вплив AI на об'єднані військові операції в повітрі, на суші і на морі;
- стратегічні наслідки AI для розгортання озброєнь і прийняття рішень щодо їх застосування.

Озброєння зі штучним інтелектом дає змогу ефективніше використовувати звичайні види озброєнь, що застосовуються в повітрі, на суші, на воді та в космосі за допомогою прийняття рішень на основі штучного інтелекту. Озброєння AI, особливо в ядерних матеріалах, токсинах і хімічних речовинах задокументовано, а також розглядається в контексті маніпулювання кліматом і використання космосу [28].

Озброєння AI в кіберпросторі є небезпечним. Якщо AI наповнювати зловмисними даними і озброїти його ядерними або іншими боєголовками, це може призвести до катастрофічних наслідків. У праці [27] визначено збройний AI як зловмисні алгоритми AI, які можуть погіршити продуктивність і порушити нормальне функціонування доброякісних алгоритмів AI, забезпечуючи при цьому сценарії технологічних атак як у кіберпросторі, так і в фізичному просторі.

Слід погодитися, що далеко не завжди AI служить засобом для досягнення раціональних цілей. Наприклад, застосування технологій штучного інтелекту у

військовій сфері цілком може призвести до катастрофічних наслідків планетарного масштабу. AI дійсно робить людину значно потужнішою, але ця потуга цілком може призвести і до смерті людства, що навряд чи буде свідчити про те, що людство стало набагато розумнішим як тоді, коли воно вело війни без застосування технологій штучного інтелекту [29].

Сучасний період характеризується стрімким розвитком технологій штучного інтелекту. Людство проходить крізь фазу, коли відбувається докорінна зміна світу, продукується об'єднання людського інтелекту, творчих здібностей людини з можливостями AI, синергії людини та автономної машини. Разом із цим загострюється потреба розвитку культури AI, відповідних світоглядних та інституційних засад його застосування. Технологічні та економічні зміни, спричинені поступом «Індустрії 5.0», вимагають комплексних та багатогранних рішень, які охоплюють не лише технічні аспекти, а й законодавчі та соціальні заходи для забезпечення сталого та етичного впровадження AI в усі сфері суспільного життя.

КОНТРОЛЬНІ ПИТАННЯ

1. Розкрийте різні підходи до визначення сутності поняття «управлінське рішення».
2. Вкажіть, яким чином відбулося переосмислення концепту «війни» у працях західних дослідників наприкінці XX – початку XXI століття.
3. Наведіть визначення понять: «гібридна війна», «гібридні загрози».
4. Охарактеризуйте спектр PMESII.
5. Зазначте роль розвитку технологій AI у військових стратегіях і плануванні.

ТЕСТИ

1. Ключову роль у процесі прийняття рішень займає:
а) особа (група осіб), яка приймає рішення;
б) методологія;
в) наявні ресурси;
г) результативність.
2. Синхронізоване використання багатьох інструментів впливу, підібраних з урахуванням конкретних вразливостей у всьому спектрі соціальних функцій для досягнення синергетичних ефектів, називається:
а) гібридна війна;
б) гібридна загроза;
в) гібридний конфлікт;
г) гібридний вплив.

3. Скоординована та синхронізована дія, яка свідомо спрямована на системні вразливості демократичних держав та інститутів за допомогою широкого спектру засобів, називається:

а) гібридна війна;

б) гібридна загроза;

в) гібридний конфлікт;

г) гібридний вплив.

4. На цей час для аналізу комплексної стратегічної та оперативної обстановки НАТО використовує конструкцію PMESII, що має шість основних доменів. Вкажіть назву домена, що складається із загального обсягу виробництва, розподілу та споживання всіх товарів і послуг для країни чи організації:

а) політичний;

б) військовий;

в) економічний;

г) соціальний.

5. Вкажіть, що з переліченого відноситься до гібридних загроз:

а) синхронізоване використання різних засобів для створення розколу у суспільстві, що становить ціль;

б) стратегія латентного маніпулювання іншими державними стратегічними інтересами;

в) вплив актора на механізм прийняття рішень з метою отримання бажаного результату (рішення) ;

г) всі відповіді вірні.

РОЗДІЛ 2.
КОНЦЕПТУАЛЬНА МОДЕЛЬ ГІБРИДНИХ ЗАГРОЗ

2.1. Ландшафт гібридних загроз: передумови, елементи та структура моделі

2.2. Державні та недержавні актори, їх використання у гібридному впливі

2.1. Ландшафт гібридних загроз: передумови, елементи та структура моделі

Однією з відповідей на численні виклики, які зумовлені впливом гібридних загроз, є розробка «Концептуальної моделі гібридних загроз» («Hybrid Threats conceptual model») та опублікування у 2020 році праці [8] спільними зусиллями Об'єднаного дослідницького центру Європейської комісії (JRC) [31] та Європейського центру передового досвіду з протидії гібридним загрозам (Hybrid CoE) [32].

Об'єднаний дослідницький центр Європейської комісії (Joint Research Centre - JRC) надає незалежні, науково обґрунтовані знання, підтримуючи політику ЄС з метою позитивного впливу на суспільство [31].

Діяльність Європейського центру передового досвіду з протидії гібридним загрозам (The European Centre of Excellence for Countering Hybrid Threats - Hybrid CoE) спрямована на: проведення досліджень, аналіз гібридних загроз та методів боротьби з ними; організацію спільного навчання для країн-учасниць; проведення консультацій на стратегічному рівні між учасниками ЄС та НАТО, залучення до діалогу урядових та неурядових експертів [32].

Основні завдання «Концептуальної моделі гібридних загроз»: підвищити обізнаність, налагодити розуміння із зацікавленими сторонами, ідентифікувати ключові проблеми та прогалини в майбутніх дослідженнях.

У «Концептуальній моделі гібридних загроз» виділено чотири основні стовпи, що необхідно вивчити, щоб мати можливість повністю зрозуміти ландшафт гібридних загроз [8]:

- ворожі актори (та їхні стратегічні цілі);
- інструменти, які використовує ворожій актор;
- цільові домени (сфери);
- фази (включаючи види діяльності, що спостерігаються в кожній фазі).

Схематична візуалізація впливу гібридних загроз за «Концептуальною моделлю гібридних загроз» [8] наведена на рис. 2.1.

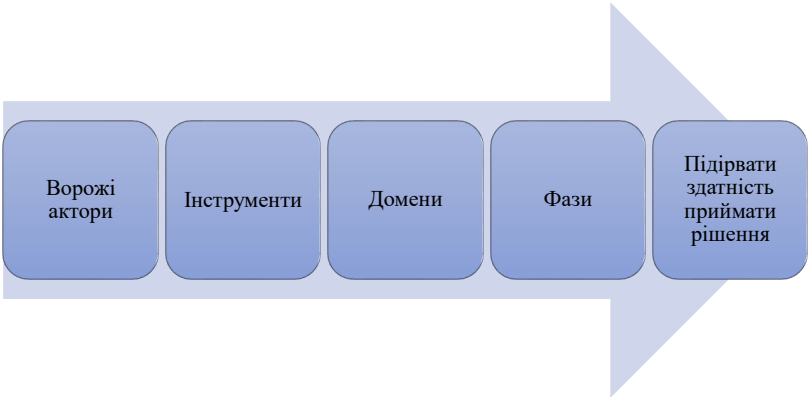

Рис. 2.1. Схематична візуалізація впливу гібридних загроз за «Концептуальною моделлю гібридних загроз»
Джерело: сформовано на основі [8], опубліковано у [33]

Так, ворожій актор (державний чи недержавний), який має цілі, але обмежені можливості для їх досягнення, може застосувати різноманітні інструменти до ряду доменів для виконання певного типу діяльності на різних фазах, щоб досягти ряд цілей і підірвати здатність приймати рішення у державі, що є ціллю (цільовій державі, державі-мішені).

2.2. Державні та недержавні актори, їх використання у гібридному впливі

Ворожій актор обирає комбінацію інструментів для досягнення стратегічних цілей. Вони утворюють набір інструментів гібридних загроз, який може відрізнятися залежно від актора, про якого йдеться (державний актор, недержавний актор) та його цілі. Кожен інструмент націлений на один або кілька доменів. Інструменти можуть використовувати або навіть створювати вразливі місця в одному чи кількох доменах. Мета може бути досягнута як прямим впливом інструменту на домен, так і за рахунок каскадних ефектів. Діяльність в одній сфері може бути спрямована на вплив у зовсім іншому домені, ніж той, де була виявлена активність [8].

Якщо за допомогою комбінації інструментів досягається бажаний ефект, це може кинути виклик суверенітету цільової держави, водночас даючи ворожому актору можливість просувати свої власні стратегічні інтереси.

Отже, актори, які вдаються до гібридної діяльності, пов’язаної з загрозами, намагатимуться вплинути на алгоритм прийняття рішень державою-мішенню. Рішення можуть бути невеликим (бізнес-угоди), локальними (електорат під час виборів) та такими, що формують політику та законодавство. Якщо операція

буде успішною, вона міститиме лише деякі аспекти, які робитимуть загрозу гібридною за своєю природою. Це означає, що дія може завдати шкоди сама по собі і її потрібно виявляти та протидіяти на ранній стадії. З цієї причини важливо вивчити акторів, які стоять за гібридною загрозою.

Діяльність, що стоїть за гібридними загрозами, здійснюється, зокрема акторами з більш-менш авторитарними або тоталітарними поглядами на владу. Мета ворожих акторів полягає в тому, щоб націлитися на демократичні системні вразливості, використовуючи всі інструменти, які є в розпорядженні авторитарної держави. Демократичні держави також можуть втручатися та впливати на діяльність інших демократичних держав, але є певні відмінності від дій авторитарних держав.

У багатьох поясненнях і визначеннях, що стосуються концепції гібридних загроз, як державні, так і недержавні актори згадуються як актори, які беруть участь у діяльності гібридних загроз з метою втручання у внутрішній простір інших держав для посилення своїх власних стратегічних інтересів, іноді навіть шляхом насильства. Різні види політик використовують гібридні загрози як механізм для просування стратегічних інтересів [8].

У «Концептуальній моделі гібридних загроз» [8] до країн, які беруть участь у діяльності гібридних загроз (державних акторів), віднесено: росію, Китай, Іран і Північну Корею. До недержавних акторів відносено: Хезболлу, Аль-Каїду та ІДІЛ. Також виокремлено маріонеткових акторів: транснаціональні організовані злочинні угруповання, ідеологічні рухи та «найманці», які працюють заради прибутку. Одним із факторів, який є спільним для акторів, є те, що всі вони так чи інакше прагнуть кинути виклик принципам верховенства права (одна з основних цінностей демократії).

У контексті гібридних загроз сьогодні найбільше обговорюють державних акторів. Однак ця концепція виникла в результаті дій, до яких були залучені слабші недержавні актори, щоб кинути виклик сильнішим сторонам за допомогою розумної тактики. Оскільки держави все ще є найпотужнішими супротивниками іншої держави чи альянсу, ми здебільшого думаємо про протидію державам у просторі гібридних загроз. Але це було б потенційно фатальним упущенням, якби до недержавних акторів не ставилися з такою ж серйозністю.

Недержавні актори в контексті гібридних загроз – це актори, які відіграють важливу роль у міжнародних відносинах і мають достатню владу, щоб втручатися, впливати та спричиняти зміни без будь-якої приналежності до встановлених інститутів держави [8]. Роль недержавних акторів змінилася разом зі змінами в міжнародній політиці в результаті глобалізації та нових зв'язків. Зміни настільки посилили їхню діяльність, що вони можуть кинути виклик національним державам і чинити тиск на демократичні уряди. Недержавні актори здійснюють вплив через втручання, іноді повільно та непомітно.

Як правило, підхід, прийнятий державами, які діють через недержавних

акторів у ворожих цілях, називається «проксі-війною» (посередницькою війною) [8].

Держави, які діють через третіх осіб з метою впливу і здійснення ворожих заходів проти інших держав, безумовно, не є новим явищем. Активний недержавний актор може набувати різноманітних форм і може проявлятися через пряму структуру іноземної держави або довгострокового союзника, сформованого через усталені відносини та взаємну залежність. Його також можна сформувати через короткостроковий альянс для досягнення спільних цілей щодо локальної чи конкретної проблеми або просто через використання «корисних ідіотів», які можуть не усвідомлювати, що вони служать меті в контексті гібридних загроз. Держави, які мають сильний і довгостроковий інтерес у впливі, маніпулюванні та створенні подій в інших країнах для просування своїх інтересів, ймовірно, намагатимуться використовувати все вищезазначене систематично.

Держави, які керують діяльністю через недержавних акторів, використовують можливість таємно здійснювати дії шкідливого характеру проти інших країн. Це має перевагу в тому, що цільовим державам стає важче виявити діяльність, розв'язану іншою країною і перешкодити цьому, а також перешкоджає здатності держави-мішені приписувати шкідливу операцію іноземній державі, яка стоїть за подією або низкою подій. Приховані дії через третю юридичну особу можуть навіть сприяти досягненню іншою державою бажаних цілей без усвідомлення державою-мішенню того, що вона стала жертвою впливу.

Держави, що діють у таємному режимі, також передбачають можливість заперечувати та спростовувати будь-які потенційні звинувачення в причетності до подій. Дуже зручним для іноземних держав, зацікавлених у здійсненні діяльності в політично чутливих сферах, є розгортання приватних військових корпорацій (ПВК) для ризикованих операцій у зонах конфлікту або для підтримки режимів, що є важливим для заперечення участі в конфлікті.

Ще одна особливість, актуальна для роботи з гібридними загрозами, – це можливість розгорнути акторів в цільовій державі з певними можливостями, що підходять для конкретних заходів. Можливість виходу на ринок у критичних секторах інфраструктури в цільовій державі була б дуже корисною перевагою для здійснення впливу та проведення обструктивних заходів, які б мали значні наслідки. Доступ до вразливих секторів у державі-мішені можна отримати шляхом прямих інвестицій існуючих підприємств або створення нових суб'єктів господарювання з конкретною ворожою метою.

Створення важелів за допомогою відкритих бізнес-структур, які часто діють у межах закону, ускладнює роботу правоохоронних органів і служб безпеки виявити такі випадки. Якщо створюються такі важелі, потрібно виділити ресурси для вжиття відповідних заходів.

Навіть злочинні організації, які діють в цільовій державі, є дуже корисними

для діяльності іноземних держав у контексті гібридних загроз. Експлуатація злочинних організацій може включати використання встановлених мереж контрабанди, здатність надавати підроблені документи, схеми фінансових злочинів або просто їх здатність погрожувати, залякувати, чинити тиск або завдавати шкоди стратегічно важливим особам чи групам у певній ситуації з політичною метою.

Експлуатація державами недержавних акторів, вбудованих у цільову державу чи цільову аудиторію, як примножувача сили, швидше за все, буде невід'ємною та зростаючою частиною прояву гібридних загроз у майбутньому .

Прогрес у соціальних медіа та кіберінструментах розширив можливості впливу на цільову аудиторію, що також може використовуватися недержавними акторами в гібридних кампаніях.

Коли шкідлива діяльність відбувається скоординовано та систематично, прояви діяльності недержавних акторів стають відчутними. Отже, визначення того, хто є ініціатором шкідливих подій, буде надзвичайно важливим для розробки відповіді на те, як протистояти цим загрозам у майбутньому.

КОНТРОЛЬНІ ПИТАННЯ

1. Охарактеризуйте основні стовпи «Концептуальної моделі гібридних загроз».
2. Визначте та охарактеризуйте основних державних ворожих акторів «Концептуальної моделі гібридних загроз».
3. Охарактеризуйте та наведіть приклади основних недержавних ворожих акторів «Концептуальної моделі гібридних загроз».

ТЕСТИ

1. Вкажіть, у якому році опубліковано «Концептуальну модель гібридних загроз»:

а) 2020;
б) 2021;
в) 2022;
г) 2023.

2. Оберіть основні стовпи, які є підґрунтям «Концептуальної моделі гібридних загроз»:

а) актори (та їхні стратегічні цілі), інструменти, які використовує актор, цільові домени, фази (включаючи види діяльності, що спостерігаються в кожній фазі);

б) актори (та їхні стратегічні цілі), цільові домени, фази (включаючи види діяльності, що спостерігаються в кожній фазі);

в) актори (та їхні стратегічні цілі), інструменти, які використовує актор, цільові домени;

г) інструменти, які використовує актор, цільові домени, фази (включаючи види діяльності, що спостерігаються в кожній фазі).

3. У «Концептуальній моделі гібридних загроз» до країн (державних акторів) віднесено:

а) росію, Китай, Іран і Північну Корею;

б) росію, Китай, Іран і Південну Корею;

в) росію, Китай, Ірак і Північну Корею;

г) Хезболлу, Аль-Каїду та ІДІЛ.

4. Суб'єкти, які відіграють значну роль у міжнародних відносинах та здатні втручатися, впливати та викликати зміни у відносинах без будь-якої належності до державних утворень називаються:

а) державні актори;

б) недержавні актори;

в) проксі-актори;

г) інтегральні актори.

5. В якості недержаних акторів можуть виступати:

а) транснаціональні організовані злочинні угруповання;

б) ідеологічні рухи;

в) приватні військові корпорації;

г) всі відповіді вірні.

РОЗДІЛ 3.
ДОМЕНИ (СФЕРИ) ГІБРИДНИХ ЗАГРОЗ

3.1. Критичні функції та вразливості
3.2. Інформаційна, кібернетична, космічна, економічна, військова/оборонна, культурна, соціальна/суспільна, державне управління, правова, розвідувальна, дипломатична, політична, інфраструктурна сфери

3.1. Критичні функції та вразливості

Гібридна загроза націлена на вплив у кількох доменах шляхом застосування комбінацій інструментів. Кожен інструмент націлений на одну або кілька сфер чи зв'язки між ними, створюючи або використовуючи вразливість. Ось чому важливо визначити сфери інтересів або критичні функції, у яких держава повинна забезпечити стійкість проти гібридних загроз, оскільки вони критично пов'язані з національною безпекою та здатністю держави приймати рішення.

При виборі доменів для «Концептуальної моделі гібридних загроз» [8] враховувалися такі основні аспекти:

- До введення концепції гібридних загроз основний підхід завжди включав військове втручання та фізичну окупацію як передумову для захоплення незалежної країни. Згідно з «Концептуальною моделлю гібридних загроз» [8] суттєвий контроль актора над ціллю може бути досягнутий без військових дій. Крім того, ворожі актори можуть використовувати стратегію гібридної загрози, щоб послабити цільовий стан без фізичного контролю. Це означає, що військово-орієнтований підхід може не дати точної картини всього спектру поточних загроз і викликів.
- Наразі не існує універсального підходу до структуризації інструментів впливу. Немає вагомих причин вибирати будь-які існуючі концепції з безлічі підходів, які використовуються паралельно і які не повністю відповідають вимогам опису гібридних загроз.
- Хоча кількість доменів (тринадцять) можна вважати великою, зменшення кількості та об'єднання їх у крупніші категорії не є суттєвим с точки зору ефективності скоординованої діяльності.
- Не менш важливим є те, що цей список базувався на рішенні групи експертів і консенсусі всередині групи, який виник під час ітераційного процесу створення «Концептуальної моделі гібридних загроз» [8]. Крім того, його було перевірено під час серії зустрічей із зовнішніми рецензентами.

Варто підкреслити, що цей список залишається відкритим і ні в якому разі не остаточним. Користувачі цієї «Концептуальної моделі гібридних загроз» [8] можуть обмежити кількість доменів, об'єднавши деякі, або збільшити кількість шляхом подальшого уточнення деталей. Точне розуміння кожної конкретної

ситуації стане основою для адекватної реакції та подолання прогалин у безпеці.

Не кожен інструмент і діяльність, що націлені на домен, можна класифікувати як гібридну загрозу. Подібним чином, не всі активи в межах домену однаково важливі для ворожого актора. Діяльність гібридної загрози, націлена на домени та використання доменів як середовища шляхом одночасного використання кількох інструментів у скоординованій кампанії, спрямованій на використання вразливостей або можливостей і на підрив процесу прийняття рішень опонентом.

Домени не слід досліджувати окремо, оскільки вплив на один домен може викликати каскадний ефект в інших. Це особливо важливо, коли розглядається вплив гібридної загрози на домен.

3.2. Інфраструктурна, кібернетична, космічна, економічна, військова/оборонна, культурна, соціальна/суспільна сфери, сфера державного управління, правова, розвідувальна, дипломатична, політична, інформаційна сфери

У «Концептуальній моделі гібридних загроз» [8] виділено та охарактеризовано тринадцять сфер:

1) Інфраструктурна сфера (інфраструктура).

Ключовим поняттям для інфраструктурної сфери є «критична інфраструктура». Надалі використовуватимемо європейське визначення «критичної інфраструктури» як «активу, системи або їх частини, розташованої в державах, що має важливе значення для підтримки життєво важливих суспільних функцій: здоров'я, безпеки, економічного чи соціального добробуту людей, і порушення або знищення якої матиме значний вплив в державі в результаті нездатності підтримувати ці функції» [34].

Незалежно від характеру ворожого актора (державного чи недержавного), інфраструктура, основні послуги та ланцюги поставок можуть бути привабливими цілями для залякування та тиску. Діяльність ворога може:

- Погіршити якість товарів та послуг.
- Здійснити руйнування ключових частин інфраструктури.
- Зменшити/усунути надмірність та спричинити залежність від ворожого актора.
- Обмежити доступ до ключових ресурсів, які необхідні для функціонування.
- Збільшити вартість експлуатації.
- Впливати на попит, створюючи тиск на інфраструктуру.

Домен інфраструктури можна розглядати як «мега-домен», оскільки він включає кілька секторів. При використанні «Концептуальної моделі гібридних загроз» [8] домен за необхідності можна розбити на декілька субдоменів.

2) Кібернетична сфера (кіберсфера).

Сьогодні кібернетичний простір відіграє виняткову та дуже специфічну роль щодо гібридних загроз. Все що відбувається в реальному світі, включаючи всі політичні та військові конфлікти, також відбувається в кіберпросторі.

З бурхливим розвитком інформаційних технологій природа загроз національній безпеці не змінюється, але кіберпростір генерує нові потужні механізми, що можуть збільшити швидкість, розповсюдження та силу атаки, а також забезпечити анонімність. Низька ціна входу, анонімність та асиметрія вразливості означають, що дрібніші актори мають більшу владу в кіберпросторі, ніж у багатьох більш традиційних сферах світової політики.

Цей домен відноситься до інформаційного середовища, що складається з взаємозалежних мереж інформаційних технологій (включаючи апаратне забезпечення, програмне забезпечення, дані, протоколи) та інформації (включаючи Інтернет, телекомунікаційні мережі, комп'ютерні системи, вбудовані процесори та контролери). Інструменти, які може застосувати ворожий актор, спрямовані на погіршення, збій або руйнування мереж. Доступ до інформації також може бути метою ворожого актора з метою збору розвідувальних даних.

3) **Космічна сфера (космос).**

Космічні послуги включають навігацію, зв'язок, дистанційне зондування, а також науку та дослідження [35]. Вплив гібридних операцій у космосі не лише впливає на військову/оборонну сферу, але також може мати значний вплив на цивільну комерційну діяльність, оскільки вона все більше покладається на космічні можливості. Насправді більшість інструментів, які націлені на космічну область, використовують зв'язок космічної сфери з іншими областями, щоб отримати каскадний ефект. Цей домен тісно пов'язаний із військовими/оборонними сферами, економікою, інфраструктурою, інформацією та розвідкою.

4) Економічна сфера (економіка).

У сучасному глобалізованому суспільстві економічні відносини за своєю суттю піддаються державним маніпуляціям і регулярно використовуються декількома країнами як першочерговий засіб у стратегічних цілях [36; 37]. У цьому контексті використовуються такі інструменти економічної політики як: санкції, оподаткування, ембарго, торговельні угоди, заморожування активів, стерилізовані інтервенції (за яких зміна іноземних активів Національного банку компенсується відповідною зміною його внутрішніх активів), субсидії, тарифи, суверенне кредитування (кредит іноземній державі, часто уряду країни, що розвивається) та прощення (анулювання) боргів [38; 39].

Метою економічної гібридної загрози є всебічне послаблення цільової держави, підриваючи довіру суспільства до демократії та уряду. Наприклад, економічні заходи або політика можуть бути використані для посилення політичного тиску [36], або економічний примус може бути спрямований на

зміну зовнішньополітичної позиції держави або послаблення стійкості її економіки, суспільства та безпеки [37].

Інструменти, пов'язані з гібридними загрозами, що намагаються вплинути на сферу економіки, є нічим іншим, як інструментами міжнародної економічної політики.

У контексті гібридних загроз сфера економіки тісно пов'язана з іншими сферами. Ці різноманітні та складні відносини в основному виникають через діяльність фірм, які можуть контролюватися або впливати на актора, схильного до використання гібридної загрози.

По-перше, залежність від енергетичної та іншої інфраструктури може породжувати економічну залежність і/або стати інструментом здійснення економічного тиску.

По-друге, розвиток інфраструктури зазвичай передбачає капітальні проєкти, які залучають прямі іноземні інвестиції (ПІІ), намір яких може бути сумнівним.

По-третє, економічні труднощі та/або нерівність можуть бути використані для впливу на результат виборів [40].

По-четверте, економічні труднощі, такі як криза платіжного балансу або зростання державного боргу, можуть використовуватися як наратив для підриву легітимності уряду або навіть для виправдання дій та/або геополітичної позиції.

По-п'яте, корупція в політичній і соціальній сферах підриває економічну безпеку, оскільки постраждала країна стає менш конкурентоспроможною на світовому ринку.

5) Військова/оборонна сфера.

У військово-оборонних операціях завданням війська є збереження незалежності, а також недоторканності та єдності території рідної країни, зокрема для підтримки та захисту суверенітету.

У мирний час військові приєднуються до цивільних органів влади для навчань і надання допомоги для того, щоб швидко реагувати на терористичні атаки, адекватно відповідати на запити цивільної влади про допомогу (у надзвичайних ситуаціях), підтримувати необхідний військовий контингент у разі нарощування сил іншої держави в безпосередній близькості від кордонів рідної країни.

Військовий і оборонний потенціал країни є основою існування держави. В новітній і давній історії наддержави поєднували економічну й військову сили та збільшували обороноздатність. Крім того, військовий потенціал є необхідною умовою для того, щоб країну сприймали як важливого гравця на глобальній геополітичній арені. Є приклади країн, які вважаються супердержавами, незважаючи на їхню економічну слабкість, тоді як інші країни з набагато сильнішою економікою та потенціалом для зростання не розглядаються через відсутність можливостей у військовій сфері. Компрометація військової та оборонної спроможності країни може бути дуже ефективним засобом посилення

впливу, здійснення тиску та підготування ґрунту для майбутніх військових операцій. Порушення військової обороноздатності країни викликає реакцію, що призводить до збільшення витрат на оборону та виснаження ресурсів. Це також неявний спосіб здійснення економічного тиску. Він також може підштовхнути ціль до ескалації, реагуючи на дії, які вважаються ворожими.

6) Сфера культури (культура).

Ця сфера передбачає використання агресором культурних цінностей для підтримки цілей гібридної діяльності. Сфера культурного державного управління може бути внутрішньою, зовнішньою або загальною. Внутрішньо культурне управління передбачає «використання культурних і цивілізаційних тем для визначення фундаментальних елементів національної ідентичності», тоді як стратегія зовнішньої політики намагається «просувати культуру як засіб створення привабливого іміджу за кордоном» [41].

7) Соціальна/суспільна сфера.

Соціальна сфера зазвичай використовується для створення, поглиблення або використання соціокультурних розколів, які породжують соціальні потрясіння, необхідні для продовження чи успішної діяльності гібридної загрози. Завжди є предметом дебатів у західних суспільствах спірні питання, такі як: безробіття, бідність і освіта. Однак питання, які можуть створити або підтримувати кризу, є особливо привабливими. Приклади включають економічний спад, нелегальну імміграцію та терористичні атаки.

Метою дій у цій сфері буде вплив на те, як працює суспільство в цільовій державі, щоб створити сприятливі умови для діяльності гібридної загрози.

8) Сфера державного управління (державне управління).

Державне управління тлумачиться як «процес перетворення державної політики на результати» [42].

Державне управління існує для виконання закону та правил. Хоча ця концепція зрозуміла в теорії, її може бути важко застосувати на практиці.

По-перше, під час тлумачення закону з метою втілення його в життя держані управлінці можуть ненавмисно робити оціночні судження, які можуть мати політичний характер.

По-друге, державне управління природно сприяє формуванню політики, оцінюючи існуючу політику та організовуючи формулювання нової.

9) **Правова сфера (право).**

Правова сфера відноситься до сукупності правових норм, дій, процесів та інститутів, включаючи як їх нормативний, так і фізичний прояв, які використовуються або можуть бути використані для досягнення юридичних або неправових наслідків у контексті кампанії гібридної загрози.

Актор може вибрати з широкого спектру правових інструментів для підтримки кампанії гібридних загроз такі, як: використання правових порогів, прогалин, складності та невизначеності; обхід своїх юридичних зобов'язань; уникнення відповідальності; посилення дотримання правил державою-мішенню;

використання відсутності юридичної сумісності між цільовими країнами; використання власних регулятивних повноважень відповідно до національного законодавства; використання закону та правових процесів для створення наративів і контрнаративів [43].

Хоча деякі з цих тактик можуть передбачати порушення норм національного або міжнародного права, не всі з них є такими. Те, що відрізняє використання закону як інструмента чи компонента гібридних загроз, полягає не в його незаконності чи нелегітимності як такій, а в таких рисах:

- Актори, які хочуть підірвати демократію, націлюються на конкретні вразливості в демократичному суспільстві за допомогою законів. Наприклад, право на свободу слова створює простір для кампаній з дезінформації.
- Закон використовується для досягнення руйнівних, диверсійних або інших пагубних наслідків проти цільової держави, що підриває її інтереси в інтересах актора.
- Закон використовується для руйнування верховенства права.
- Закон часто використовується для досягнення ефекту в інших сферах, зокрема в інформаційному просторі, тоді як діяльність в інших сферах може бути використана для досягнення ефекту в правовій сфері.

10) Розвідувальна сфера (розвідка).

«Розвідка – це процес, за допомогою якого конкретні види інформації, важливі для національної безпеки, вимагаються, збираються, аналізуються і надаються політикам; продукти цього процесу; забезпечення цих процесів і цієї інформації контррозвідувальною діяльністю; проведення операцій, як цього вимагає законна влада» [44]. Розвідка надає тим, хто приймає рішення, обізнаність про ситуацію, необхідну для прийняття стратегічних рішень і рішень, пов'язаних із безпекою. Таким чином, розвідувальна діяльність повинна бути розроблена та реалізована для задоволення потреб або передбачена політичними вказівками.

Актор, який використовує гібридні загрози, може використовувати розвідку двома основними способами. Зазвичай актори використовують власні розвідувальні можливості для підтримки запланованих або поточних гібридних загроз або можуть спробувати вплинути на розвідувальні операції цільової держави. В обох випадках актор прагне підірвати здатність держави-мішені контролювати ситуацію.

Розвідка може підтримуватися і використовуватися для підтримки широкого спектру гібридних загроз. Її можна вважати пов'язаною з усіма іншими доменами. Тим не менш, розвідка має міцний зв'язок з інформаційною сферою тому, що спецслужби можуть організовувати чи сприяти кампанії з дезінформації.

Ця сфера також тісно пов'язана з кібернетичною та космічною сферами. Метою розвідувальної підтримки діяльності з гібридною загрозою є підрив можливостей прийняття рішень на політичному рівні і здатності державного

управління реалізовувати політику, незалежно від того, використовується вона для здійснення таємних операцій на підтримку діяльності гібридної загрози чи для розмивання ситуаційної обізнаності цільової держави та/або створення обману.

11) Дипломатична сфера (дипломатія).

Зовнішня політика традиційно зосереджена на безпеці [45]. Насправді нормативні теорії міжнародних відносин виправдовують війну як захисний захід проти спровокованої агресії з урахуванням обмежень пропорційності та захисту цивільних [46].

Діяльність гібридних загроз, особливо у сфері дипломатії, спрямована на створення розбіжностей на державному чи міжнародному рівнях, підтримка будь-яких інформаційних кампаній і втручання в процес прийняття рішень. Гібридні загрози в дипломатії: дипломатичні санкції, бойкоти, використання посольств і створення заплутаних або суперечливих наративів.

Домен дипломатії має тісні зв'язки з політичною сферою. Хоча зовнішню політику, як правило, розглядають окремо від внутрішньої політики, вони дуже тісно взаємопов'язані, через потребу учасників переговорів у міжнародній політиці, щоб їхні рішення були ратифіковані їхніми виборцями. В авторитарних державах зовнішня політика полягає в підтримці внутрішньої політики. Область дипломатії в цьому випадку стає майже полем битви за домовлену реальність.

Окрім тісного зв'язку з внутрішньою політикою, дипломатія в контексті гібридних загроз також пов'язана з економічною, соціальною та правовою сферами. Дипломатичні санкції та бойкоти спрямовують серйозний вплив на економіку держави-мішені.

12) Політична сфера (політика).

У контексті гібридних загроз політична сфера охоплює акторів, організації та інституції, які мають владу чи правлять на території шляхом застосування різних форм політичної влади та впливу [47].

Ворожі актори можуть спробувати використати політичну сферу, щоб вплинути на державу-мішень або створити сприятливі умови для здійснення гібридної загрозливої діяльності. Політична влада може використовуватися або всередині країни, або на дипломатичній арені. В останньому випадку діяльність може бути окремою або поєднувати політичну владу різних акторів для досягнення більшого ефекту. Інструменти цього домену спрямовані на демократичні процеси, політичні організації та осіб.

Політична сфера тісно пов'язана з дипломатією через здатність зовнішньої політики сильно впливати на внутрішню політику. Відносини між ними часто описують як «дворівневу гру» [48]. Ця сфера також тісно пов'язана з державним управлінням, оскільки останнє існує для реалізації державної політики, але також може впливати на формування політики.

Крім того, деякі інструменти політичної сфери використовуються для зміни сприйняття громадськістю політичного вибору та/або акторів. Таким чином,

інструменти інформаційної сфери можна використовувати для підтримки гібридних загроз, спрямованих на політичну область.

Крім того, якщо актори хочуть уникнути відкритої конфронтації, вони намагатимуться використати юридичні прогалини та діяти в межах національного і міжнародного права. У цьому сенсі саме правова сфера формує середовище, в якому актор може спробувати використовувати політичну сферу.

Нарешті, успіх кількох інструментів у цій сфері залежить від прихованого характеру залучених дій. Тому актори, що стоять за гібридною загрозою, використовують свої розвідувальні служби, які здатні організовувати та проводити таємні операції.

13) Інформаційна сфера (інформація).

Використання інформації як зброї залишається характерною рисою гібридних загроз. Її використовують, щоб підірвати уявлення про безпеку людей, протиставляючи політичні, соціальні та культурні ідентичності одна одній. Мета інформаційної гібридної загрози полягає в тому, щоб використати політику ідентичності та лояльності, таким чином розділивши впливові групи інтересів і політичні альянси. З'являється плутанина і безлад, оскільки люди почуваються більш невпевнено. Завдяки своїй низькій інтенсивності та потенціалу заперечення дії гібридної загрози, ця сфера загалом має низький ризик, допускається підхід методом проб і помилок, подібно до гнучких процесів, що використовуються в технологічних компаніях. Інформаційні гібридні загрози мають відносно низьку вартість та деякі відкриті для аутсорсингу.

Кібердезінформація, чорна пропаганда, фейкові новини — це неправдива інформація, яка також має на меті створити враження, що її створили ті, кого вона має дискредитувати. Зазвичай використовується, щоб очорнити, збентежити або спотворити когось. Фейкові новини в соціальних мережах - це не просто публікації, яким поставили лайк, поділилися чи підписалися, а скоріше, потужна техніка примноження кіберпропаганди. Інтернет – це джерело інформації, яке можна вважати дуже критичним.

Інструменти цього домену спрямовані на зміну політичного дискурсу, створення або просування наративів і маніпулювання громадською думкою та настроями. Крім того, вони можуть порушувати свободу поглядів і вираження. Свобода вираження поглядів включає повагу до свободи та плюралізму засобів масової інформації, а також права громадян мати свою думку, отримувати і поширювати інформацію та ідеї «без втручання з боку державної влади та незалежно від кордонів» [49]. Однак очікується, що органи державної влади в демократичних країнах почнуть навчати громадян щодо загрози дезінформації та захищатимуть їх від дій, спрямованих на маніпулювання їхніми поглядами та рішеннями.

Інформаційна сфера тісно пов'язана з культурною та соціальною/суспільною сферами, оскільки кампанії з дезінформації та інші інструменти в цій сфері прагнуть вплинути на однорідність культури та

суспільства цільової держави. На це також впливає домен розвідки оскільки інформація, отримана за допомогою кібернетичного чи традиційного шпигунства, може слугувати для впливу на громадську думку, сприйняття та дискурс. Крім того, оскільки однією з цілей інформаційної сфери є підрив політичної дискусії та процесів у цільовій державі, вона також може бути пов'язана з політичною сферою.

КОНТРОЛЬНІ ПИТАННЯ

1. Охарактеризуйте інфраструктурний домен «Концептуальної моделі гібридних загроз».
2. Охарактеризуйте кібернетичний та космічний домени «Концептуальної моделі гібридних загроз».
3. Охарактеризуйте економічний домен «Концептуальної моделі гібридних загроз».
4. Охарактеризуйте військово/оборонний та розвідувальний домени «Концептуальної моделі гібридних загроз».
5. Охарактеризуйте культурний та соціальний/суспільний домени «Концептуальної моделі гібридних загроз».
6. Охарактеризуйте домен державного управління та правовий домен «Концептуальної моделі гібридних загроз».
7. Охарактеризуйте дипломатичний та політичний домени «Концептуальної моделі гібридних загроз».
8. Охарактеризуйте інформаційний домен «Концептуальної моделі гібридних загроз».

ТЕСТИ

1. «Актив, система або їх частина, розташована в державах, що має важливе значення для підтримки життєво важливих суспільних функцій: здоров'я, безпеки, економічного чи соціального добробуту людей, і порушення або знищення якої матиме значний вплив в державі в результаті нездатності підтримувати ці функції» називається:
а) критична інфраструктура;
б) кібернетичний простір;
в) космічна сфера;
г) розвідка.
2. Діяльність ворожого актора на домен інфраструктури може бути спрямована на:
а) зменшення вартості експлуатації;
б) розширення доступу до ключових ресурсів;

в) зменшення/усунення надмірності та спричинення залежності від ворожого актора;

г) побудову ключових частин інфраструктури.

3. Вкажіть сферу, що передбачає використання агресором культурних цінностей для підтримки цілей гібридної діяльності:

а) державного управління;

б) культурна сфера;

в) політична сфера;

г) соціальна/суспільна сфера.

4. «Процес перетворення державної політики на результати» відноситься до сфери:

а) державного управління;

б) правової сфери;

в) політичної сфери;

г) сфери дипломатії.

5. «Процес, за допомогою якого конкретні види інформації, важливі для національної безпеки, вимагаються, збираються, аналізуються і надаються політикам; продукти цього процесу; забезпечення цих процесів і цієї інформації контррозвідувальною діяльністю; проведення операцій, як цього вимагає законна влада», називається:

а) критична інфраструктура;

б) кібернетичний простір;

в) космічна сфера;

г) розвідка.

РОЗДІЛ 4.
ІНСТРУМЕНТИ ГІБРИДНИХ ЗАГРОЗ

4.1. Система інструментів гібридного впливу

Відповідно до «Концептуальної моделі гібридних загроз» [8] у кожному домені є способи, за допомогою яких ворожий актор може досягти ефекту. Більш того, цей ефект може охоплювати різні домени, оскільки вони пов'язані один з одним. За результатами узагальнення сукупності інструментів та здійснення вибірки тих, що стосуються різних сфер, орієнтовний список інструментів, які можуть бути використані ворожим актором для досягнення своєї мети, впливаючи на відповідні сфери, наведено у табл. 4.1.

Таблиця 4.1

Розподіл інструментів гібридних загроз за сферами

Сфера	Інструменти
Інфраструктура	Фізичні операції проти інфраструктури Створення та використання залежності від інфраструктури (включаючи цивільно-військову залежність) Прямі іноземні інвестиції Промислове шпигунство Кібершпигунство Кібероперації Сприяння соціальним заворушенням Використання порогових станів, неможливість атрибуції, прогалини та невизначеність у законодавстві Використання правових норм, процесів та інститутів Контроль та втручання в ЗМІ Електронні операції (заглушення та спуфінг GNSS)
Кіберсфера	Фізичні операції проти інфраструктури Створення та використання залежності від інфраструктури (включаючи цивільно-військову залежність) Прямі іноземні інвестиції Промислове шпигунство Кібершпигунство Кібероперації Використання порогових станів, неможливість атрибуції, прогалини та невизначеність у законодавстві Використання правових норм, процесів та інститутів Дезінформаційні кампанії та пропаганда Електронні операції (заглушення та спуфінг GNSS)

Продовження табл. 4.1

Сфера	Інструменти
Космічна сфера	Фізичні операції проти інфраструктури Створення та використання залежності від інфраструктури (включаючи цивільно-військову залежність) Прямі іноземні інвестиції Промислове шпигунство Кібершпигунство Кібероперації Використання порогових станів, неможливість атрибуції, прогалини та невизначеність у законодавстві Використання правових норм, процесів та інститутів Електронні операції (заглушення та спуфінг GNSS)
Економічна сфера	Фізичні операції проти інфраструктури Створення та використання залежності від інфраструктури (включно із цивільно-військовою залежністю) Створення або використання економічних залежностей Прямі іноземні інвестиції Промислове шпигунство Підрив національної економіки Використання економічних труднощів Сприяння соціальним заворушенням Сприяння та використання корупції Використання порогових станів, неможливість атрибуції, прогалини та невизначеність у законодавстві Використання правових норм, процесів та інститутів Дипломатичні санкції, бойкоти Електронні операції (заглушення та спуфінг GNSS)
Військова/оборонна сфера	Фізичні операції проти інфраструктури Створення та використання залежності від інфраструктури (включаючи цивільно-військову залежність) Прямі іноземні інвестиції Кібершпигунство Кібероперації Порушення повітряного простору Територіальне порушення водних ресурсів Розповсюдження зброї Збройні сили -звичайні/надзвичайні операції Воєнізовані організації Військові навчання Використання порогових станів, неможливість атрибуції, прогалини та невизначеність у законодавстві Використання правових норм, процесів та інститутів Підготовка розвідувальної інформації Підпільна діяльність Проникнення Електронні операції (заглушення та спуфінг GNSS)

Продовження табл. 4.1

Сфера	Інструменти
Сфера культури	Залучення діаспор для впливу Фінансування культурних груп і аналітичних центрів Експлуатація соціокультурних розколів (етнічних, релігійних, культурних) Маніпулювання дискурсами щодо міграції для поляризації суспільства та підрив ліберальної демократії Вплив на навчальні програми та академічні кола Використання порогових станів, неможливість атрибуції, прогалини та невизначеність у законодавстві Використання правових норм, процесів та інститутів Контроль та втручання в ЗМІ Дезінформаційні кампанії та пропаганда
Соціальна/суспільна сфера	Фізичні операції проти інфраструктури Кібероперації Порушення повітряного простору Територіальне порушення водних ресурсів Військові навчання Залучення діаспор для впливу Фінансування культурних груп і аналітичних центрів Експлуатація соціокультурних розколів (етнічних, релігійних, культурних) Сприяння соціальним заворушенням Маніпулювання дискурсами щодо міграції для поляризації суспільства та підрив ліберальної демократії Використання вразливих місць у державному управлінні (включаючи управління надзвичайними ситуаціями) Вплив на навчальні програми та академічні кола Сприяння та використання корупції Використання порогових станів, неможливість атрибуції, прогалини та невизначеність у законодавстві Використання правових норм, процесів та інститутів Посольства Створення плутанини або суперечливого наративу Міграція як розмінна монета в міжнародних відносинах Дискредитація керівництва та/або кандидатів Підтримка політичних акторів Використання імміграції для політичного впливу Контроль та втручання в ЗМІ Дезінформаційні кампанії та пропаганда

Продовження табл. 4.1

Сфера	Інструменти
Сфера державного управління	Фізичні операції проти інфраструктури Створення та використання залежності від інфраструктури (включаючи цивільно-військову залежність) Створення або використання економічних залежностей Прямі іноземні інвестиції Підрив національної економіки Використання економічних труднощів Кібершпигунство Кібероперації Використання вразливих місць у державному управлінні (включаючи управління надзвичайними ситуаціями) Сприяння та використання корупції Використання порогових станів, неможливість атрибуції, прогалини та невизначеність у законодавстві Використання правових норм, процесів та інститутів Дискредитація керівництва та/або кандидатів Підтримка політичних акторів Примус політиків та/або уряду Дезінформаційні кампанії та пропаганда
Правова сфера	Прямі іноземні інвестиції Маніпулювання дискурсами щодо міграції для поляризації суспільства та підрив ліберальної демократії Сприяння та використання корупції Використання порогових станів, неможливість атрибуції, прогалини та невизначеність у законодавстві Використання правових норм, процесів та інститутів Примус політиків та/або уряду
Розвідка	Прямі іноземні інвестиції Промислове шпигунство Залучення діаспор для впливу Використання порогових станів, неможливість атрибуції, прогалини та невизначеність у законодавстві Використання правових норм, процесів та інститутів Підготовка розвідувальної інформації Підпільна діяльність Проникнення Посольства
Дипломатія	Створення або використання економічних залежностей, Підрив національної економіки Використання економічних труднощів, Порушення повітряного простору Територіальне порушення водних ресурсів Військові навчання Залучення діаспор для впливу Фінансування культурних груп і аналітичних центрів

Закінчення табл. 4.1

Сфера	Інструменти
	Використання порогових станів, неможливість атрибуції, прогалини та невизначеність у законодавстві Використання правових норм, процесів та інститутів Дипломатичні санкції, бойкоти Посольства Міграція як розмінна монета в міжнародних відносинах
Політика	Створення або використання економічних залежностей Прямі іноземні інвестиції Підрив національної економіки Використання економічних труднощів Порушення повітряного простору Територіальне порушення водних ресурсів Військові навчання Залучення діаспор для впливу Фінансування культурних груп і аналітичних центрів Сприяння соціальним заворушенням Маніпулювання дискурсами щодо міграції для поляризації суспільства та підрив ліберальної демократії Використання вразливих місць у державному управлінні (включаючи управління надзвичайними ситуаціями) Використання порогових станів, неможливість атрибуції, прогалини та невизначеність у законодавстві Використання правових норм, процесів та інститутів, Дипломатичні санкції, бойкоти Посольства Міграція як розмінна монета в міжнародних відносинах Дискредитація керівництва та/або кандидатів Підтримка політичних акторів Примус політиків та/або уряду Використання імміграції для політичного впливу Дезінформаційні кампанії та пропаганда
Інформаційна сфера	Фізичні операції проти інфраструктури Прямі іноземні інвестиції Промислове шпигунство Залучення діаспор для впливу Використання порогових станів, неможливість атрибуції, прогалини та невизначеність у законодавстві Використання правових норм, процесів та інститутів Створення плутанини або суперечливого наративу Контроль та втручання в ЗМІ Дезінформаційні кампанії та пропаганда

Джерело: сформовано на основі [8]

Кожен інструмент не обов'язково є гібридною загрозою. Наприклад, кібероперація може бути як частиною гібридної загрози, так і не бути нею. Тому

варто говорити, що «гібрид – це завжди комбінація інструментів, але не всі комбінації є гібридними» [8].

4.2. Приклади інструментів гібридних загроз

У кожному домені були описали способи, за допомогою яких ворожий актор може впливати. Крім того, вплив може охоплювати різні домени, оскільки вони тісно пов'язані один з одним.

На рис. 4.1 наведено приклади інструментів, які може використовувати ворожий актор для ураження певних доменів задля досягнення своїх цілей.

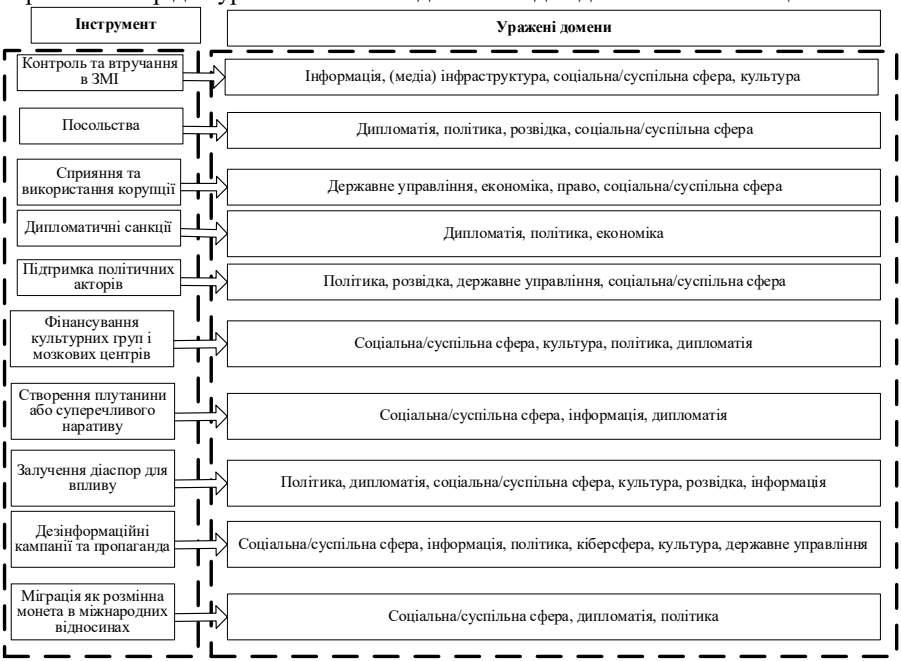

Рис. 4.3. Приклади інструментів, які може використовувати ворожий актор для ураження певних доменів за «Концептуальною моделлю гібридних загроз»
Джерело: сформовано на основі [8]

Відповідно до «Концептуальної моделі гібридних загроз» [8] для досягнення власних цілей ворожий актор може застосовувати широкий спектр інструментів, які впливають як безпосередньо, так і опосередковано на сфери впливу гібридних загроз. Наведемо приклади застосування деяких інструментів.

Контроль та втручання в ЗМІ втілюється у контролі за інформаційним ресурсом та формуванням завдяки йому необхідної реакції громадськості та презентації «обраних» лідерів громадської думки.

Посольства як створення центрів збору інформації та організації агентури.

Корупція може бути використана як інструмент для:

- дестабілізації економіки. Високий рівень корупції може призвести до зменшення іноземних інвестицій, зростання ризику та витрат для бізнесу, а також зменшення довіри населення до власної економіки. Це може призвести до зменшення рівня зайнятості та поширення бідності.

- здійснення політичного впливу. Корупція може призвести до зменшення ефективності політичної системи та зниження рівня довіри населення до уряду та до державних інституцій, збільшення соціальних протиріч та створення роздробленості в суспільстві. Це може призвести до зростання впливу зовнішніх сил, які можуть використовувати цю ситуацію у своїх власних інтересах.

Дипломатичні санкції – припинення дипломатичних відносин між державами, обмеження дипломатичної присутності.

Підтримка політичних акторів – створення так званої «п'ятої колони», тобто проросійськи налаштованих політиків, громадських діячів тощо.

Фінансування культурних груп та аналітичних центрів (діаспора, культурні фонди, культурні товариства, мистецькі організації, релігійні об'єднання тощо), що займаються розповсюдженням наративів, які загострюють або штучно створюють антагоністичні протиріччя та конфліктні ситуації.

Створення плутанини або суперечливого наративу – маніпулювання навколо історичних постатей та подій, художні інтерпретації історії, за допомогою чого підмінюють (викривляють) поняття та сутність подій.

Залучення діаспор для впливу на політику держави в якості інструмента дестабілізації у суспільстві.

Дезінформаційні кампанії та пропаганда втілюються у формі вироблення культурних продуктів, контент яких містить необхідні наративи.

Міграція як розмінна монета в міжнародних відносинах передбачає використання мігрантів як інструменту тиску або дискредитації.

КОНТРОЛЬНІ ПИТАННЯ

1. Охарактеризуйте систему інструментів гібридного впливу «Концептуальної моделі гібридних загроз».
2. Наведіть приклади інструментів, які може використовувати ворожий актор для досягнення своїх цілей у різних доменах.

ТЕСТИ

1. Розповсюдження зброї, звичайні операції збройних сил, воєнізовані організації (проксі) - це інструменти, які уражають:

а) військово-оборонний домен;

б) розвідку;

в) політичний домен;

г) інфраструктурний домен.

2. Оберіть інструмент, який уражає дипломатичну, політичну та економічну сфери:

а) дипломатичні санкції;

б) сприяння та використання корупції;

в) дезінформаційні кампанії та пропаганда;

г) промислове шпигунство.

3. Оберіть інструмент, який уражає сферу державного управління, економічну, правову, соціальну/суспільну сфери:

а) дипломатичні санкції;

б) сприяння та використання корупції;

в) дезінформаційні кампанії та пропаганда;

г) промислове шпигунство.

4. Оберіть інструмент, який уражає кіберсферу, сферу державного управління, соціальну/суспільну, інформаційну, політичну, культурну сфери:

а) дипломатичні санкції;

б) сприяння та використання корупції;

в) дезінформаційні кампанії та пропаганда;

г) промислове шпигунство.

5. Фізичні операції проти інфраструктури, прямі іноземні інвестиції, промислове шпигунство, залучення діаспор для впливу, використання порогових станів, неможливість атрибуції, прогалини та невизначеність у законодавстві, використання правових норм, процесів та інститутів, створення плутанини або суперечливого наративу, контроль та втручання в ЗМІ, дезінформаційні кампанії та пропаганда – це інструменти, які будуть ефективними для ураження:

а) військово/оборонного домену;

б) культурного домену;

в) інформаційного домену;

г) інфраструктурного домену.

РОЗДІЛ 5.
ДИНАМІКА ГІБРИДНИХ ЗАГРОЗ

5.1. Роль різних видів діяльності в ландшафті гібридних загроз

Гібридні загрози є всеохоплюючою концепцією, яка включає широкий спектр дій. Ця частина «Концептуальної моделі гібридних загроз» [8] прояснює роль різних видів діяльності в ландшафті гібридних загроз: втручання, вплив, кампанії та війна.

На основі вивчення літератури, що стосується зміни характеру війни та того, як змінюється безпекове середовище, стає зрозуміло, що існують різні типи діяльності з різним ступенем інтенсивності, тривалі часові рамки та змінена географія в поєднанні з тим фактом, що ворожі актори, можуть мати певні причини (наприклад, матеріальні) ведення такої політики. Вони діють у тіні або в сірій зоні між прийнятним і неприйнятним, законним і незаконним, поєднуючи вплив з інструментами для зміцнення своїх зусиль.

Різні типи діяльності гібридних загроз у «Концептуальній моделі гібридних загроз» [8] поміщено на часову шкалу, що вказує на те, що існує потенціал ескалації гібридних загроз, який охоплює як короткострокові, так і довгострокові можливості. Хронологія має три різні фази, а саме: підготовка, дестабілізація та примус. Всі фази мають сильну психологічну складову. Спектр дій, зокрема, втручання, вплив, кампанії та війна на різних етапах збігаються.

Ескалація може бути присутня чи відсутня. Також може спостерігатися деескалація, що означає, що діяльність також може згортатися, плутаючи факти та маскуючи справжні цілі дії. Це характерно для ландшафту гібридних загроз. Ескалація та деескалація можуть бути горизонтальними та вертикальними, їхня комбінація і спосіб їх використання пристосовується до ситуації та потреб.

Для розуміння гібридної війни була розроблена «Аналітична модель для розуміння гібридної війни» [14], що фокусується на вразливих місцях захисника, здатності нападника в гібридній війні синхронізувати широкий спектр своїх можливостей під час атаки, а також на ефектах, створених в результаті цих дій проти конкретних вразливостей його наміченої цілі (рис. 5.1). «Аналітична модель для розуміння гібридної війни» [14] складається з трьох взаємозалежних частин:

– критичні функції та вразливості захисника;

– синхронізоване використання зловмисником декількох засобів та використання горизонтальної ескалації;

– лінійні та нелінійні ефекти від гібридних атак.

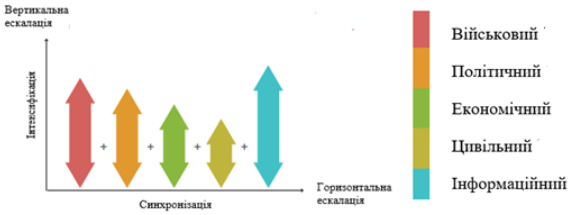

Рис. 5.1. Ескалація гібридної війни

Джерело: [14]

На рис. 5.1 показано, як актор гібридної війни може синхронізувати свої військові, політичні, економічні, цивільні, інформаційні (military, political, economic, civilian, informational – MPECI) інструменти впливу для вертикальної і горизонтальної ескалації через низку конкретних дій для досягнення ефекту. Вона також показує, як актор гібридної війни може здійснювати вертикальну ескалацію, збільшуючи інтенсивність одного або багатьох інструментів впливу, та/або горизонтальну «ескалацію» через синхронізацію декількох інструментів впливу для створення ефектів більших, ніж при вертикальній ескалації [14].

Ключовим моментом є розуміння того, що різні інструменти впливу використовуються в різних вимірах і на різних рівнях одночасно і синхронізовано. Такий тип мислення дозволяє актору гібридної війни використовувати різні засоби MPECI, що є в їхньому розпорядженні, для створення синхронізованих пакетів атак, які спеціально пристосовані до передбачуваних вразливостей цільової системи-мішені. Інструменти впливу, що використовуються, залежать від можливостей ворожого актора і вразливостей держави-мішені, а також від політичних цілей актора гібридної війни і запланованих ним шляхів досягнення цих цілей.

5.2. Фази гібридних загроз, гібридні види діяльності

У «Концептуальній моделі гібридних загроз» [8] виділено та охарактеризовано три фази:

1) **Підготовка (праймінг).**

На етапі підготовки (праймінгу) кінцева мета ворожого актора полягає в тому, щоб ціль добровільно зробила шкідливий вибір і прийняла рішення. Якщо на цій стадії вже є план, який передбачає ескалацію до військового конфлікту, ворожий актор намагатиметься проникнути та спрямувати свої можливості у внутрішній простір держави-мішені. Ця мета досягається через втручання, яке розмиватиме ситуаційну обізнаність. На цей момент в актора вдосталь стратегічного терпіння. У дослідженнях безпеки та військових досліджень фазу

підготовки часто називають праймінг (попередньою підготовкою).

Попередня підготовка передбачає серію дій, які здійснюються в очікуванні бою чи тактичної операції, спрямованої на сприяння досягненню стратегічних цілей. Сенс таких дій полягає в тому, щоб підвищити успіх шляхом заперечення або пом'якшення потенційно несприятливих ефектів, одночасно посилюючи потенційно сприятливі фактори. «Це означає, що така діяльність зосереджена на будь-якому факторі або комбінації факторів, які можуть вплинути на результат, і може залучати будь-які або всі ешелони тактичної кампанії» [50]. Навіть підготовка та формування заходів у сфері безпеки і військової підготовки у випадку гібридних загроз має бути, оскільки ворожі актори (авторитарні держави) мають взаємопов'язані відносини з військовими та розвідкою.

Праймінг краще підходить до природи гібридних загроз, оскільки він також враховує цивільне населення, яке є ключовим і як ціль, і для протидії гібридним загрозам.

Навіть якщо діяльність із самого початку була розрахована на уникнення відкритого конфлікту чи війни, все одно спрацьовує ефект примноження сил, що стоять за цією діяльністю, який ґрунтується на військовому мисленні, типовому для стратегічної культури авторитарної держави, де влада залежить від розвідувальних служб та військових.

Психологічний вплив тягне за собою трансформацію свідомості та моделі поведінки цільової особи чи групи**,** в результаті чого маніпулювання певним суспільством або спільнотою, їх визначальними властивостями, поглядами, цінностями та спільними нормами підштовхне державу-мішень прийняти рішення, бажане агресору.

Ідея праймінгу полягає в тому, що він матиме довгостроковий вплив на поведінку окремої людини, групи чи організації. Техніка праймінгу полегшує тестування культурних факторів шляхом з'ясування того, що є помітним і доступним для учасників у момент, коли рішення прийнято, та що може впливати на поведінку. Схоже, існує певний рівень згоди серед соціальних психологів, «що це простий вплив на соціально значущі стимули, які можуть сприяти або стимулювати безліч суджень, цілей і дій, часто навіть за межами намірів або усвідомлення людей» [51].

Механізм праймінгу включає два компонента:

- «збудження» - представлення у пам'яті певним процесом, поширюючи активацію через семантичну мережу асоціацій;
- використання доступних представлень для кодування інформації про соціальну ціль, яка була отримана згодом [51].

Праймінг важливий під час початкової фази в інформаційній, культурній, дипломатичній, політичній, суспільній, кібернетичній, розвідній, економічний та державній сферах.

Ще одна часто згадувана сфера – кіберсфера. Діяльність у кіберпросторі може завдати шкоди інфраструктурі, тоді як збір інформації шляхом злому, різні

типи збоїв і перевантаження також є частиною набору інструментів для пошуку способів посилення впливу. Праймінг також може бути націлений на окремих людей або на різні типи спільнот, особливо тих, які не відчувають себе причетними до країни, в якій вони проживають. Більше того, у міжнародних відносинах спроби втручання та порушення існуючих норм з метою отримання більшого впливу належать до початкової фази.

Дії, які пов'язані з економічними факторами, також можуть бути частиною цього виду діяльності. Створення важелів впливу за допомогою економічних засобів має давнє коріння. Для шляхів здійснення впливу можуть використовуватися: умови, що стосуються позик [52], прямі іноземні інвестиції (ПІІ), право власності на майно чи бізнес.

Важливим є питання впливу. Вплив є частиною звичайної державної політики, і більшість держав намагаються впливати на міжнародну політику. Однак існує два види впливу: відкритий (звичайний) із чіткими цілями та вплив, який є частиною гібридних загроз, який часто називають гібридним впливом. У міжнародній політиці впливові держави здатні ефективно використовувати ширший портфель інструментів впливу, щоб змінити переконання та поведінку інших держав. Саме ця здатність лежить в основі ефективного державного управління, що захищає та просуває національні інтереси у сучасному глобалізованому світі [53]. З погляду гібридних загроз державне управління, яке ґрунтується на ресурсах і відкрито оголошує цілі впливу на інші держави, є звичайним способом спроби посилити вплив.

З точки зору гібридних загроз, управління державою – це здатність творчо та економічно ефективно поєднувати різні засоби для посилення впливу без прямих переговорів з іншою державою. Методи спочатку спрямовані на населення, місцевий рівень та інституційний рівень через втручання, а потім, як тільки актору вдається вклинитися у внутрішній простір держави-мішені, він починає проводити прихований вплив. Це може принести бажаний результат повільніше, але з більш тривалим ефектом.

Отже, вплив створюється за допомогою різних форм втручання, яке в деяких випадках може навіть включати використання військової сили у формі порушення повітряного простору та військових навчань.

Втручання може ще не бути гібридною діяльністю як такою. Діяльність починає ставати гібридною, коли починає відповідати критеріям гібридних загроз. Коли випаде нагода чи необхідність, створений вплив буде використано. На цьому етапі діяльність стане більш помітною, а також гібридною. Навіть якщо загрозу виявлено, шкоду вже завдано і стає важче реагувати та стримувати активність.

У деяких випадках бажаний ефект може бути досягнутий навіть наприкінці фази праймінгу. Якщо це так, ефект буде досягнутий шляхом прийняття рішення цільовою державою у спосіб, який буде вигідним для агресора. Зрештою, це виявляється ефективною тактикою і її буде дуже важко приписати справжньому

ворожому актору, що стоїть за всією діяльністю, через синергетичний ефект сукупності інструментів і доменів, що розмиває ситуаційну обізнаність.

2) **Дестабілізація через операції та кампанії.**

Фаза дестабілізації – це стадія, на якій актор активізує свою діяльність у вигляді кампанії (кілька операцій) для досягнення поставленої мети [8].

На відміну від фази праймінгу, що має на меті в основному щось отримати, як-от: інформація, позиціонування, тестування інформації, навчання або перевага – у фазі дестабілізації є заздалегідь запланована мета.

Важко визначити, коли ворожий актор перемикає режим. У фазі дестабілізації діяльність стає більш помітною, агресивною та включає більше насильства. Це відбувається відповідно до потреб актора чи можливостей. На цій фазі діяльність розширює межі прийнятного і неприйнятного, а також законних і незаконних дій. Однією з цілей ворожого актора у використанні механізму, що стоїть за гібридними загрозами, є розпад фіксованих категорій порядку [54]. Це означає, що є багаторівневі дії, спрямовані на дестабілізацію функціонуючої держави та поляризацію її суспільства [55]. Це було б неможливо без фази підготовки.

Навіть якщо діяльність стає більш помітною, офіційного визнання з боку актора не буде («правдоподібне заперечення»), і може бути дуже важко надати докази. Коли діяльність базується на секретній інформації, складно зібрати публічну та відкриту доказову базу. Це явна перевага для ворожого актора, який стоїть за діяльністю. Тут інформація та суспільні сфери є відносно вільним простором для дій. Якщо дискусії та дебати, пов'язані з подіями, проводяться у відкритому доступі, а інформація та факти засекречені, демократичні держави стають аутсайдерами, а ідея «влада слабких» починає діяти.

На етапі дестабілізації можуть спостерігатися більш енергійні наративні просування, явна дезінформація та пропаганда, а також активація ботів, кібератак (перевантаження державних і приватних служб, блокування та встановлення шкідливих програм тощо). Крім того, он-лайн перетворюється в оф-лайн, тобто коли щось, що просувалося у віртуальному світі, стає активним у формі протестів чи заворушень. Ці більш відкриті та агресивні дії спрямовані на дестабілізацію цільового суспільства. У деяких випадках суспільство, що зазнає впливу, використовується для впливу на реальну ціль як запланований ефект другого порядку (де увага зосереджена в одному місці, але справжня ціль знаходиться в іншому). Сьогодні Європа застосовує цю ідею дестабілізації разом з ідеями, що лежать в основі використання діяльності, пов'язаної з гібридними загрозами. Тут теж присутня ідея, щоб через інші рівні впливати на державу, підштовхуючи до прийняття неправильних рішень.

Крім того, дестабілізаційна діяльність використовує різні зв'язки між сферами, які зазвичай розглядаються як окремі, але які в сучасному середовищі безпеки тісно взаємопов'язані та переплетені. Це включає в себе зв'язки між зовнішньою та внутрішньою безпекою, зв'язки на державному та місцевому

рівнях, уявлення про друзів і ворогів, цивільно-військові зв'язки, сфери юрисдикції різних органів влади, різні правові рамки, віртуальний світ проти реального світу та навіть розуміння війни й миру. У цих зв'язках діяльність гібридної загрози знову може стосуватися багатьох різних сфер, включаючи правову, інформаційну, військову, суспільну, політичну, економічну, космічну, інфраструктурну, кіберсферу та сферу державного управління.

І якщо праймінг пов'язаний з реагуванням, то у фазі дестабілізації потрібно вже говорити про необхідність і реагувати, і захищатися. Під час цієї фази міжсекторальна реакція буде неадекватною, оскільки актор, який стоїть за діяльністю, діє відповідно до довгострокових стратегічних інтересів, навіть якщо мета здається короткостроковою.

Під час фази дестабілізації відбувається свідомий поштовх до прийняття рішень під тиском. Тепер ворожий актор знає, чого хоче, є чітка мета: діловий договір; результат голосування (вибори та референдуми); рішення на рівні ЄС чи НАТО; перешкоджання двосторонній угоді; блокувати, відкладати або скасовувати рішення про використання військових; рішення щодо режимів санкцій; будь-яке багатостороннє рішення; стратегічні рішення країни приєднатися або відмовитися від альянсів або нормативних міжнародних правил тощо. Усі короткострокові цілі пов'язані з довгостроковими стратегічними цілями. При прийнятті вищезазначених типів рішень ідеальною основою для прийняття рішення буде правильна обізнаність про ситуацію та широка інформація, а також можливість оцінити різні перспективи. Насправді це трапляється рідко, і ситуація стає ще складнішою, якщо ворожий актор чинить тиск.

Якщо бажаного ефекту не досягнуто, діяльність ворожого актора або повертається до підготовки (праймінгу) - він чекає іншої можливості, підбирає кращу комбінацію чи створює нові вразливості, або ж починається фаза. Це залежить від кількох факторів: важливості стратегічних цілей, реакції та подальших можливостей.

3) **Примус через гібридну війну.**

Остання фаза – примус. Діяльність тепер вийшла за межі недооцінки, її можна назвати гібридною війною. Гібридна війна представляє «важкий кінець» спектру ескалації діяльності гібридних загроз. В основному гібридна війна – це комбінація таємних і відкритих військових операцій у поєднанні з політичними та економічними заходами, підривною діяльністю, операціями з дезінформації, пропаганди та фейковими новинами, таємним чи відкритим розгортанням спеціальних сил, а також військовою допомогою, або відкрита військова діяльність. Дії включають кібератаки як невід'ємну частину.

Хоча на цій фазі потенційно використовуються всі стратегічні сфери (політика, дипломатія, розвідка, інформація, військова/оборонна сфера, економіка, інфраструктура, культура, право, соціальна/суспільна сфера, державне управління, кіберсфера і космос), гібридна війна включає застосування

сили як її основний елемент. Від терору, диверсій і підривної діяльності до партизанської війни, звичайної війни і навіть ядерної сфери. Усі можливі рівні ескалації можна включити або навіть поєднати. У зв'язку з цим застосування сили є не лише додатковим елементом в гібридних загрозах, вона також змінює всю концепцію конфлікту, перетворюючи його на війну. На цій фазі концепція діяльності - це «акт сили, щоб змусити ворога виконувати власну волю» [56].

По суті, можна стверджувати, що такий вид війни не є чимось новим. Така боротьба часто включає стратегію і тактику асиметричної війни, коли слабша сторона намагається використати стратегію для компенсації кількісних або якісних недоліків у своїх силах і обладнанні. Це відрізняє її від симетричної або військово-орієнтованої війни, де дві держави мають порівнянну військову міць і ресурси та покладаються на тактику, яка в цілому схожа, відрізняючись лише деталями та виконанням.

Згідно з дослідженням війни [57]:

1) слабші сторони перемогли в більш ніж 30% усіх досліджених війн;

2) існує тенденція до того, що слабші сторони все більше перемагають.

Ті, хто веде гібридну війну, зазвичай певним чином є слабшими акторами, це держави чи актори, які уникають відкрито оголошеної війни. Таким чином, це може перерости у війну між воюючими сторонами, чия військова міць та тактика суттєво відрізняються. Як правило, це конфлікт між постійною професійною армією та повстанцями чи рухом опору, які часто мають статус учасників незаконних бойових дій.

Особливість бойової активності в просторі гібридної загрози була розроблена таким чином, щоб здійснити новий виклик і включати елемент несподіванки, оскільки «гібридна війна - це не стандартизоване поєднання різних типів протистоянь, а інколи неорганізований, спрямований опір, який не слідує військовій тактиці, але створює власне середовище війни, зазвичай повністю ігноруючи будь-які правила» [58].

Діяльність гібридної війни як частина ландшафту гібридних загроз є продуктом XXI ст., який використовує нові можливості, створені змінами в середовищі безпеки, як наприклад, конкуренція за новий статус; розвиток джерел живлення; нові типи мереж і взаємозалежностей; зміни у збройних формуваннях; зрушення в наративах від політичної ідеології до морального популізму та окремих питань, які кидають виклик демократичній державній системі; умисне насильство проти мирного населення з метою дестабілізації; технологічні інновації, які також уможливлюють кібердіяльність і новий інформаційний простір.

Таким чином, навіть якщо коріння війни залишалося незмінним протягом століть, а ідеї про те, як виграти війну, слідують схожим моделям, війна все ще розвивається. Поточні зміни в середовищі безпеки завжди впливатимуть на стратегічне мислення та привнесуть нові особливості в загальний простір безпеки.

«Концептуальна модель гібридних загроз» [8] охоплює ключові елементи, які формують ландшафт гібридних загроз: актори, які застосовують гібридні механізми, фази гібридної кампанії, інструменти та цільові домени (сфери) для досягнення стратегічних цілей ворожого актора.

Концептуалізація гібридних загроз забезпечує контекст і основу для подальшого розвитку концепції гібридних загроз на академічному, політичному та оперативному рівнях.

КОНТРОЛЬНІ ПИТАННЯ

1. Охарактеризуйте «Аналітичну модель для розуміння гібридної війни».
2. Зазначте фази та різні види діяльності в «Концептуальній моделі гібридних загроз».
3. Охарактеризуйте фазу праймінгу «Концептуальної моделі гібридних загроз».
4. Охарактеризуйте фазу дестабілізації «Концептуальної моделі гібридних загроз».
5. Охарактеризуйте фазу примусу «Концептуальної моделі гібридних загроз».

ТЕСТИ

1. Вкажіть, які інструменти впливу актор гібридної війни може синхронізувати для вертикальної і горизонтальної ескалації в «Аналітичній моделі для розуміння гібридної війни»:

а) військові, політичні, економічні, цивільні, інфраструктурні;
б) політичні, економічні, цивільні, інформаційні, інфраструктурні;
в) військові, політичні, цивільні, інформаційні, інфраструктурні;
г) військові, політичні, економічні, цивільні, інформаційні.

2. Вкажіть, на якій фазі кінцева мета ворожого актора полягає в тому, щоб ціль добровільно зробила шкідливий вибір і прийняла рішення, називається:

а) фаза дестабілізації;
б) фаза праймінгу;
в) фаза примусу;
г) фаза ескалації.

3. Фаза, на якій актор активізує свою діяльність у вигляді кампанії (кілька операцій) для досягнення поставленої мети, називається:

а) фаза дестабілізації;
б) фаза праймінгу;
в) фаза примусу;
г) фаза ескалації.

4. Вкажіть, на якій фазі концепція діяльності ворожого актора – це акт сили, щоб змусити ворога виконувати власну волю:

а) фаза дестабілізації;

б) фаза праймінгу;

в) фаза примусу;

г) фаза ескалації.

5. Вкажіть, які види діяльності використовує ворожий актор у «Концептуальній моделі гібридних загроз»:

а) втручання, вплив, кампанії та горизонтальна ескалація;

б) втручання, вплив, кампанії та вертикальна ескалація;

в) втручання, вплив, кампанії та війна;

г) втручання, вплив, кампанії та ескалація.

РОЗДІЛ 6.
ОСНОВИ ЗАХИСТУ

6.1. Історія питання та основні підходи до протидії гібридним загрозам
6.2. Концепція комплексної безпеки (на прикладі фінської моделі)
6.3. Самооцінка; протидія; моніторинг та виявлення гібридних загроз; стримування; реагування
6.4. Принципи побудови механізмів захисту від гібридних загроз

6.1. Історія питання та основні підходи до протидії гібридним загрозам

Концепція гібридної загрози набула поширення у зв'язку з діями росії в Україні і кампаніями ІДІЛ, що виходять далеко за межі Сирії і Іраку. Зіткнувшись з цим викликом, що постійно еволюціонує, Європейський союз і НАТО здійснили низку кроків для посилення своїх можливостей і досягнення спільних цілей через тіснішу співпрацю. Спільна декларація ЄС і НАТО (далі – Документ), ухвалена в липні 2016 року на полях Варшавського саміту НАТО, є чітким кроком уперед у цьому напрямку. Документ окреслює нові сфери практичної співпраці, зокрема щодо гібридних загроз, розбудови стійкості у сфері кібербезпеки та стратегічних комунікацій. У висновках Ради ЄС від 6 грудня 2016 року підкреслено, що імплементація спільної декларації є ключовим політичним пріоритетом для ЄС. Рада привітала прогрес, досягнутий у поглибленні відносин між ЄС і НАТО, в тому числі, у впровадженні та введенні в дію паралельних процедур і сценаріїв взаємодії у протидії гібридним загрозам. З метою забезпечення подальшого прогресу Рада схвалила спільний набір пропозицій, спрямованих на поліпшення координації, ситуаційної обізнаності, стратегічної комунікації, реагування на кризи і посилення стійкості. Північноатлантична рада схвалила такий же набір заходів [59].

В ЄС доволі чітко ідентифікували «гібридні загрози» та визначали заходи протидії. З протидії гібридним загрозам Євросоюз тісно взаємодіє з НАТО (табл. 6.1).

Таблиця 6.1

Документи ЄС щодо ідентифікації та протидії гібридним загрозам

Документ, джерело	Визначення
Спільний рамковий документ з протидії гібридним загрозам (06.04.2016р.) [60]	зазначено, що ключові виклики миру і стабільності лежать у східному і південному сусідстві ЄС.
Глобальна стратегія ЄС «Спільне бачення, Спільна дія: Сильніша Європа» (28.06.2016р.) [61]	визначає, що «на сході був порушений європейський безпековий порядок», та вказує причину – «порушення росією міжнародного права та дестабілізація України».

Закінчення табл. 6.1

Документ, джерело	Визначення
Спільна доповідь Європейському парламенту і Європейській Раді з його імплементації (19.07.2017р.) [62]	підкреслюється, що «загрози все більше набувають неконвенційних форм».
Спільний робочий документ «Східне партнерство – 20 очікуваних досягнень до 2020 року: фокусуючись на головних пріоритетах та реальних результатах» (15.12.2016р.; 13.06.2017р.) [63]	гібридні загрози концептуально визначено як «поєднання примусової та підривної діяльності, традиційних і нетрадиційних методів (тобто дипломатичних, військових, економічних, технологічних), які можуть бути скоординовано використані державними чи недержавними суб'єктами для досягнення конкретних цілей, залишаючись на рівні нижче порогу формально оголошеної війни».
Спільна заява Президента Європейської Ради, Президента Європейської Комісії і Генерального секретаря НАТО (липень 2016 р.) [64]	першим завданням визначено «підвищення здатності протидіяти гібридним загрозам»
Доповідь Європейського парламенту «Протидія гібридним загрозам: Співпраця ЄС-НАТО» (березень 2017р.) [65]	гібридну війну визначено як «ситуацію, у якій країна вдається до відкритого використання збройних сил проти іншої країни на додаток до комбінації інших засобів (тобто економічних, політичних та дипломатичних)», а гібридну загрозу як «явище, яке виникає внаслідок конвергенції та взаємозв'язку різних елементів, які разом утворюють більш складну та багатовимірну загрозу».

Джерело: складено на основі [60-66]

Слід відмітити, що поряд з прийняттям важливих програмних документів створено і нині функціонує ряд організацій, метою діяльності яких є проведення досліджень з питань генезису та трансформування гібридних загроз, напрацювання методів, засобів та механізмів для протидії цим загрозам, організація спільного навчання та консультацій для країн-учасниць тощо (табл. 6.2).

Таблиця 6.2

Хронологія створення організацій, метою діяльності яких є проведення досліджень з питань генезису та трансформування гібридних загроз

Період започаткування	Організація/ документ, характеристика
Січень 2014 року	Розпочато функціонування Центру передового досвіду з питань стратегічних комунікацій (The NATO Strategic Communications Centre of Excellence). Центр здійснює науково-аналітичну, навчально-методичну та інформаційно-комунікативну діяльність. Ним розроблено низку спеціальних навчальних курсів зі стратегічних комунікацій; видається

Продовження табл. 6.2

Період започаткування	Організація/ документ, характеристика
	журнал «Стратегічні комунікації у сфері оборони» (Defence Strategic Communications); здійснюються дослідження; проводяться конференції та семінари за такими темами, як наприклад: роль пропаганди в сучасному світі, російська інформаційна війна проти України, маніпулятивні техніки, перетворення соціальних медіа на зброю, практика НАТО щодо стратегічних комунікацій тощо.
Вересень 2015 року	Розпочала роботу оперативна робоча група зі стратегічних комунікацій Європейського Союзу - East StratCom Task Force. Діяльність групи спрямована на роз'яснення ключових аспектів політики Європейського Союзу, створення його позитивного іміджу та протидії дезінформації тощо.
Квітень 2016 року	Єврокомісія ухвалила «Спільні принципи протидії гібридним загрозам - відповідь Європейського Союзу» (Joint Framework on countering hybrid threats a European Union response). У Спільних принципах наголошується на необхідності вироблення державами-членами узгоджених механізмів реалізації стратегічних комунікацій для протидії дезінформації та публічного викриття гібридних загроз. У документі зазначається, що важливо захищати об'єкти критичної інфраструктури (наприклад, транспорт і телекомунікації), оскільки гібридні атаки можуть призвести до серйозних економічних або соціальних порушень. Документ визначає, що діяльність у сфері стратегічних комунікацій передбачає тісну взаємодію з НАТО. Зазначається, що співпраця ЄС та НАТО дозволить обом організаціям більш ефективно реагувати на гібридні загрози.
Листопад 2016 року	Європейський парламент прийняв Резолюцію «Стратегічні комунікації Європейського Союзу як протидія пропаганді третіх сторін» (EU strategic communication to counteract propaganda against it by third parties). Ухвалений документ ґрунтується на нормативних актах Європейського Союзу, прийнятих раніше, зокрема на Плані дій щодо стратегічних комунікацій (Action Plan on Strategic Communication).
Травень 2017 року	У ЄС досить серйозно підійшли до виявлення гібридних загроз і запропонували створити Центр аналізу гібридних загроз ЄС (EU Hybrid Fusion Cell) в рамках Розвідувального і ситуативного центру ЄС (EU Intelligence and Situation Centre, EU INTCEN) Європейської служби зовнішньої дії. Саме на цю нову структуру, яка у травні 2017 року набула повної оперативної здатності, і покладено завдання збору, аналізу і доведення відкритої та закритої інформації стосовно індикаторів та попереджень про гібридні загрози. Цей Центр підводить гібридні загрози під єдиний європейський знаменник та доводить відомості про них, у тому числі й у формі «Гібридного Бюлетеня» (Hybrid Bulletin), до інституцій ЄС і країн-членів Євросоюзу.
Вересень 2017 року	У Фінляндії працює Європейський центр протидії гібридним загрозам (The European Centre of Excellence for Countering Hybrid Threats). Метою Центру є протидія «новим загрозам, спрямованим на дестабілізацію ситуації в європейських країнах».

Закінчення табл. 6.2

Період започаткування	Організація/ документ, характеристика
	Діяльність Центру спрямована на: проведення досліджень, аналіз гібридних загроз та методів боротьби з ними; організацію спільного навчання для країн-учасниць; проведення консультацій на стратегічному рівні між учасниками ЄС та НАТО, залучення до діалогу урядових та неурядових експертів.

Джерело: складено за даними [66-67]

Функціонування зазначених вище організацій та реалізація прийнятих документів дозволить сприяти запобіганню та виявленню гібридних загроз, зокрема посилити боротьбу з тероризмом та організованою злочинністю, підвищити стійкість критичної інфраструктури до кібератак, сприяти науковим дослідженням та інноваціям, розвитку системи освіти тощо .

Країни-джерела гібридних загроз, як визначають в ЄС, можуть використовувати вразливих членів суспільства, нав'язуючи їм радикальні та екстремістські ідеї через сучасні канали комунікації (пропаганда). Тому в інформаційній сфері Євросоюз ключовим завданням визначив підвищення рівня обізнаності суспільства та протидії пропаганді. Була створена Спеціальна група «Стратком Схід» (East Stratcom Task Force), запущений спеціальний проект EU-STRAT, який працює й по країнам Східного партнерства, а вилучення нелегального інформаційного контенту покладається, зокрема на Антитерористичний інтернет-центр ЄС у складі Європолу. У кібер-сфері ЄС схвалив Стратегію кібер-безпеки ЄС, Європейський порядок денний безпеки, Директиву з мережевої й інформаційної безпеки. Окремо Єврокомісія створила Агентство ЄС із мережевої й інформаційної безпеки (ENISA) для протидії кібер-загрозам на рівні ЄС та Платформу мережевої й інформаційної безпеки (NIS Platform) для взаємодії органів ЄС з громадськими та приватними гравцями у кібер-просторі. Важливо відзначити, що в енергетичній сфері в якості протидії гібридним загрозам у Спільному рамковому документі визначена необхідність диверсифікації джерел і шляхів постачання енергоресурсів до ЄС, перш за все — розвиток Південного газового коридору для поставок каспійського газу і створення хабів скрапленого газу. З метою захисту критично важливої інфраструктури діє Європейська програма захисту критично важливої інфраструктури (EPCIP), а Європейське оборонне агентство працює над визначенням необхідних можливостей захисту. Для протидії гібридним загрозам у військовій сфері ЄС обмежився посиленням розвідки, розвитком відповідних можливостей із захисту критичної інфраструктури і протидії використанню мініdронів [66].

Члени НАТО стикаються із загрозами і викликами з боку як державних, так і недержавних акторів, які використовують гібридні дії для нападу на політичні

інститути, впливу на громадську думку і підриву безпеки громадян країн НАТО. Гібридні методи ведення війни - такі як пропаганда, обман, саботаж та інші невійськові тактики - вже давно використовуються для дестабілізації супротивників. Новим в атаках, які спостерігаються останніми роками, є їх швидкість, масштаб і інтенсивність, чому сприяють швидкі технологічні зміни і глобальна взаємопов'язаність. НАТО має стратегію щодо своєї ролі в протидії гібридній війні і готова захищати Альянс і усіх членів Альянсу від будь-якої загрози – як звичайної, так і гібридної. Основна відповідальність за реагування на гібридні загрози або атаки покладається на країну-мішень [68]:

- члени НАТО посилюють свою національну стійкість, в тому числі, проти гібридних загроз, і покращують свою здатність розуміти картину гібридних загроз в Альянсі, зокрема витончені гібридні стратегії, що застосовуються рф і Китайською Народною Республікою;

- НАТО готова допомогти будь-якому члену Альянсу протистояти гібридним загрозам в рамках колективної оборони. Альянс розробив стратегію своєї ролі в протидії гібридній війні, яка допоможе протистояти цим загрозам;

- з 2016 року Альянс публічно заявляє, що гібридні дії проти одного або кількох членів Альянсу можуть призвести до рішення застосувати статтю 5 Північноатлантичного договору;

- у липні 2018 року лідери НАТО домовились про створення груп контргібридної підтримки, які надаватимуть членам Альянсу на їх запит індивідуальну цілеспрямовану допомогу в підготовці до гібридних дій і реагуванні на них;

- у липні 2022 року лідери НАТО схвалили комплексні варіанти запобігання і реагування на гібридні загрози. Вони можуть бути адаптовані до конкретних ситуацій;

- НАТО посилює свою координацію з партнерами, в тому числі, з Європейським союзом, у зусиллях з протидії гібридним загрозам;

- Об'єднаний відділ розвідки і безпеки НАТО має відділ гібридного аналізу, який допомагає поліпшити обізнаність про ситуацію;

- Альянс активно протидіє дезінформації і пропаганді - не більше пропаганди, а більше фактів - онлайн, в ефірі і в друкованих виданнях.

Безпека є наскрізною проблемою, яка стосується всіх сфер життя. Тому потрібно розробляти й впроваджувати всі можливі інструменти та важелі для побудови надійної екосистеми безпеки в усьому світі.

6.2. Концепція комплексної безпеки (на прикладі фінської моделі)

Концепція комплексної безпеки – це фінська модель готовності, в якій влада, бізнес, неурядові організації та громадяни несуть спільну відповідальність за захист життєдіяльності суспільства. Мета полягає в тому, щоб під час кризи все фінське суспільство могло швидко мобілізувати ресурси, де це необхідно,

швидко відновитися і адаптувати свої функції на основі отриманих уроків. Коріння концепції - в доктрині «Тотальної оборони» після Другої світової війни, коли все суспільство мобілізувалося як частина військових оборонних зусиль [69].

Базові засади Концепції комплексної безпеки описані в Стратегії безпеки суспільства (2017) [70]. Модель ґрунтується на спільній відповідальності всього суспільства перед суб'єктами на всіх рівнях (табл. 6.3).

Таблиця 6.3

Загальні принципи комплексної безпеки (на прикладі фінської моделі)

Принципи	Характеристика
Демократія та верховенство права	Комплексна безпека ґрунтується на недоторканності людської гідності, принципах представницької демократії, поділу влади, законності використання публічної влади та інших принципах верховенства права. Права особи повинні гарантуватися в усіх ситуаціях, а органи влади повинні бути наділені достатніми повноваженнями.
Розподіл повноважень ґрунтується на моделі компетентних органів влади	Розподіл повноважень ґрунтується на визначених законом завданнях та обов'язках компетентних органів влади. Інші суб'єкти безпеки підтримують компетентні органи.
Всі суб'єкти повинні бути залучені - комплексне використання ресурсів суспільства	Життєво важливі функції забезпечуються ефективним і всебічним використанням ресурсів суспільства. Це вимагає співпраці між державним сектором, бізнес-операторами, організаціями та іншими органами, а також громадянами та координації дій у всіх ситуаціях. Необхідно забезпечити достатній обсяг ресурсів для забезпечення готовності. Економічна ефективність досягається шляхом розробки та координації процедур і систем, що використовуються у звичайних умовах, з тим, щоб їх можна було застосовувати і під час інцидентів.
Готовність підтримується форумами співпраці щодо забезпечення комплексної безпеки	Компетентні органи можуть розраховувати на підтримку широких форумів співробітництва, які сприяють плануванню на випадок надзвичайних ситуацій та забезпеченню готовності. На практичному рівні це включає зустрічі керівників служб готовності та постійних секретарів (на рівні Уряду), Комітету з питань безпеки (за підтримки Уряду) та Національного агентства з постачання на випадок надзвичайних ситуацій (як агентства, що підтримує і розвиває безпеку постачання Фінляндії). Компетентним органам влади також надають підтримку комітети з питань готовності окремих міністерств і відомств, регіональні комітети з питань готовності та управлінські групи з муніципального планування готовності.
Передбачення, гнучкість і відновлення	Завдяки комплексним заходам із забезпечення готовності можна більш ефективно передбачати ризики та гнучко використовувати ресурси. Метою планування процесу відновлення є забезпечення кращої стійкості до процесу відновлення та вищого рівня готовності.

Закінчення табл. 6.3

Принципи	Характеристика
Рівень ЄС та міжнародний вимір готовності	Життєво важливі функції суспільства та загрози для них є частиною глобального операційного середовища. Кожна життєво важлива функція суспільства має вимір на рівні ЄС і на міжнародному рівні, коли для них розробляються заходи з забезпечення готовності. Процес формування картини ситуації підкреслює необхідність посилення співпраці на рівні ЄС та міжнародному рівні. Зобов'язання, викладені в законодавстві ЄС та міжнародних угодах, які є обов'язковими для Фінляндії, враховуються в заходах з підвищення готовності.
Моніторинг та розвиток готовності	Готовність систематично контролюється і розвивається за допомогою таких інструментів, як аудит і навчання. Використання дослідницької інформації, результатів розслідувань, пов'язаних з безпекою, та застосування рекомендацій, наданих у них, сприяють розвитку готовності.
Поширення інформації про безпеку	Інформація про роботу із забезпечення готовності та безпеки повинна бути максимально доступною наскільки це можливо. Однак, з міркувань безпеки, не вся інформація може бути широко поширюватися.

Джерело: складено на основі [70]

Життєво важливі для суспільства функції повинні бути захищені в будь-який час – як в нормальних умовах, так і в кризових ситуаціях. У стратегії безпеки суспільства життєво важливі функції є основою для забезпечення готовності.

В основі Стратегії безпеки суспільства (2017) [70] лежать сім функцій, життєво важливих для суспільства:

1. Лідерство. Забезпечення лідерства є життєво важливим, оскільки воно створює основу для захисту всіх інших функцій. Функціонування керівництва має бути забезпечене в усіх ситуаціях і на всіх оперативних рівнях. Ефективне реагування на інциденти вимагає тісної співпраці між сторонами, відповідальними за надання картини ситуації і за комунікацію.

2. Міжнародна діяльність та діяльність в ЄС. Міжнародна діяльність охоплює всі рівні та сектори фінського суспільства. Забезпечення основи для міжнародного співробітництва та участь у запобіганні криз є невід'ємною частиною захисту інших життєво важливих функцій суспільства. Співпраця у сфері безпеки на рівні ЄС є невід'ємною частиною планування безпеки в адміністративних галузях.

3. Обороноздатність. Фінляндія захищатиме свою незалежність і територіальну цілісність, підтримуючи і розвиваючи оборонний потенціал, адаптований до її безпекового середовища, а підтримка оборонного потенціалу Фінляндії полягає у створенні системи стримування проти застосування військової сили і загрози застосування військової сили. У разі необхідності

Фінляндія буде відбивати військові загрози, спрямовані проти неї, за допомогою військової сили.

4. Внутрішня безпека. Підтримуючи внутрішню безпеку, Фінляндія може запобігати і протидіяти злочинній діяльності проти неї та її населення, а також запобігати нещасним випадкам, шкоді навколишньому середовищу та іншим подібним інцидентам і загрозам і успішно справлятися з їхніми наслідками. Ця робота підтримується тісною співпрацею між іншими національними і міжнародними органами влади, Європейським Союзом і суб'єктами на всіх адміністративних рівнях.

5. Економіка, інфраструктура та безпека постачання. Забезпечення функціонування економіки, інфраструктури та безпеки постачання допомагає захистити фінансові та інші ресурси для життєдіяльності. Внутрішня та міжнародна інфраструктура, організації, структури та процеси, необхідні для життєдіяльності, є захищеними.

6. Функціональна спроможність населення та послуг. Функціональна спроможність населення та його добробут забезпечуються шляхом збереження ключових базових послуг. Вони допомагають забезпечити незалежне життя в будь-яких ситуаціях.

7. Психологічна стійкість. Психологічна стійкість означає здатність окремих осіб, громад, суспільства і нації витримувати тиск, що виникає в результаті кризових ситуацій, і відновлюватися від їх наслідків. Хороша психологічна стійкість полегшує процес відновлення.

Однак жодну з них не слід розглядати як окремий об'єкт, оскільки всі функції тісно переплетені між собою. Загрози для однієї функції впливають на інші функції.

Готовність є ключовим елементом забезпечення життєво важливих функцій. У своїй основі вона означає діяльність і запобіжні заходи, що забезпечують операційну спроможність під час збоїв, які виникають у звичайних умовах і під час надзвичайних ситуацій.

Ключові висновки з фінської моделі готовності [69]:

1) У забезпеченні готовності кожен відіграє свою роль: Уряд відповідає за загальну картину і координацію зусиль із забезпечення життєдіяльності, органи влади, муніципалітети та інші державні органи співпрацюють для забезпечення безперервності надання послуг. Неурядові організації надають послуги, координують участь волонтерів у заходах на підтримку органів влади. Приватний сектор відіграє все більш важливу роль у процесі забезпечення готовності, оскільки бізнес працює на об'єктах критичної інфраструктури суспільства. Пули, що діють при Національному агентстві з надзвичайних ситуацій, об'єднують суб'єктів приватного та державного секторів для посилення співпраці та стійкості. До них відносяться, наприклад, Пул цифрових послуг, Технологічний пул, Пул громадського здоров'я та Медіа-пул.

2) Збройні сили Фінляндії організовують курси національної оборони з 1961 року, а курси регіональної оборони - з 1962 року. Регіональні курси оборони наразі організовуються спільно з обласними державними адміністраціями. Курси оборони дають цивільному і військовому персоналу загальне уявлення про зовнішню, безпекову і оборонну політику Фінляндії, а також про організацію, готовність і розвиток різних секторів національної оборони і решти суспільства в умовах кризових ситуацій і конфліктів мирного і воєнного часу. Оборонні курси поглиблюють розуміння всеосяжної безпеки та покращують співпрацю між різними секторами суспільства та державними установами. На курсах слухачі дізнаються про комплексну безпеку, стійкість, національну готовність, національне законодавство та процеси прийняття рішень. Курси готують слухачів до співпраці та до дій у різних видах криз, а не лише у збройних конфліктах.

3) Національне постачання на випадок надзвичайних ситуацій має глибоке коріння в історії фінської готовності та комплексної безпеки. Протягом останніх десятиліть основи постачання на випадок надзвичайних ситуацій змістилися від накопичення товарів до забезпечення безперебійного надання критично важливих послуг. Фінське постачання на випадок надзвичайних ситуацій базується на двох ключових елементах: Фонд надзвичайних ситуацій, який дозволяє швидко реагувати на різноманітні надзвичайні ситуації та кризи, та широка мережа державних і приватних організацій, які працюють над питаннями, пов'язаними з готовністю та безперебійним наданням послуг.

4) Залучення приватного сектору до забезпечення готовності суспільства є життєво важливим, оскільки приватні структури виконують функції, які є критично важливими для суспільства. Мета полягає в тому, щоб забезпечити безперервне функціонування суспільства в цілому під час заворушень і кризових ситуацій. Приватний сектор, що працює у сфері критично важливих послуг, добровільно та активно бере участь у різного роду навчаннях разом з органами влади з метою підвищення своєї стійкості.

5) Галузеві пули, де бізнес і державний сектор обмінюються інформацією, беруть участь у навчаннях і налагоджують зв'язки, також відіграють життєво важливу роль у контексті ситуаційної обізнаності. Актуальна та всебічна ситуаційна обізнаність має вирішальне значення при оцінці наслідків суспільних заворушень та кризових ситуацій. Під час складних і взаємопов'язаних криз, таких як COVID-19 і війна в Україні, де глобальні мережеві ланцюги поставок відіграють важливу роль, потреба у співпраці між державними та приватними структурами у формуванні всебічної ситуаційної обізнаності багато в чому є життєво важливою.

6) Концепція 72 годин [71], яка деталізує рівень готовності до надзвичайних ситуацій, рекомендований владою та неурядовими організаціями для фінських домогосподарств. Наприклад, тривале відключення електроенергії може призвести до ситуації, коли суспільні послуги будуть порушені або навіть

припинені. Домогосподарствам слід бути готовими до самостійного існування протягом щонайменше трьох днів у разі перебоїв у постачанні електроенергії. Вони повинні мати принаймні триденний запас продуктів харчування та медикаментів. Також важливо знати основи готовності, наприклад, звідки отримувати достовірну інформацію під час перебоїв і як виживати в будинку, де стає все холодніше і холодніше. Готовність до надзвичайних ситуацій приносить велику користь як суспільству, так і, перш за все, кожній окремій людині. Ось чому кожен повинен бути готовим до збоїв та надзвичайних ситуацій. Ось як кожен може підготуватися.

Фінська модель комплексної безпеки є багато в чому унікальною. Вона була пристосована до конкретних потреб і можливостей Фінляндії з моменту закінчення Другої світової війни і скоригована відповідно до змін у безпековому ландшафті Фінляндії – адже війна в Україні заклала основи для застосування Фінляндією принципів і правил НАТО.

6.3. Самооцінка; протидія; моніторинг та виявлення гібридних загроз; стримування; реагування

Гібридні дії характеризуються неоднозначністю, що створюється шляхом поєднання традиційних і нетрадиційних засобів - дезінформації і втручання в політичні дебати або вибори, порушення критичної інфраструктури, кібернетичні напади, різні форми злочинної діяльності і, нарешті, асиметричне використання військових засобів і ведення війни. Все це актуалізує необхідність посилення протидії гібридним загрозам. Один з підходів щодо формування системи протидії гібридним загрозам детально описаний у роботі [72] (рис. 6.1).

«Система протидії гібридній війні» [72] розпочинається із постановки реалістичних стратегічних цілей, починаючи від: збереження здатності до самостійних дій; переконання або стримування супротивника від гібридної агресії; шляхом зриву або запобігання подальшій гібридній агресії супротивника.

Потім доцільно визначати відповідні пороги для вжиття заходів. Вони можуть відрізнятися залежно від типу агресії або вразливості, на яку спрямована загроза, та здатності до протидії.

Далі необхідно розробити та реалізувати стратегію, засновану на трьох компонентах [72]:

1) Виявляти. Цей компонент в першу чергу вирішує проблему виявлення гібридних загроз або атак. Це вимагає оновлення попереджувальної розвідки для моніторингу «відомих невідомих» за допомогою індикаторів та попереджень та виявлення «невідомих невідомих» за допомогою розпізнавання образів та передбачення.

2) Стримувати. Цей компонент стосується стримування гібридних агресорів. Його реалізація вимагає спирання на традиційне стримування для

здійснення надійних заходів шляхом творчої горизонтальної ескалації, адаптованої та доведеної до агресора, які врівноважені між стримуванням через заперечення, включаючи стійкість і покарання.

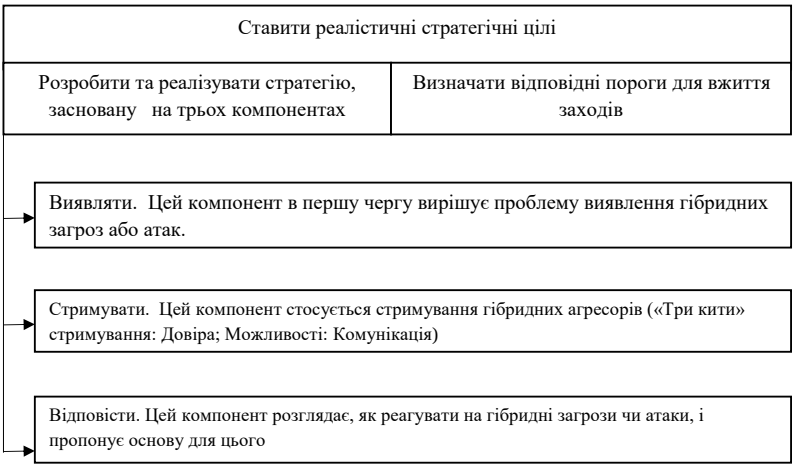

Рис. 6.1. «Система протидії гібридній війні»
Джерело: сформовано на основі [72]

Ефективне стримування гібридних агресорів тримається на «трьох стовпах» – довірі, можливостях, комунікації за допомогою здійснення таких обов'язкових дій [72]:

а) Довіра:

- Розробіть численні креативні, низькорівневі горизонтальні варіанти відплати через важелі впливу MPECI, які є політично досяжними, але демонструють чітку рішучість.
- Підсильте тих, хто сприяє таким діям стримування, як обізнаність громадськості про загрози.
- Готуйтеся до колективного стримування і багатонаціональних дій за допомогою інституційних механізмів в очікуванні гібридного нападу .
- Встановіть чіткі пороги для відповіді та дотримуйтеся їх – забезпечте послідовність риторики та дій, але також подумайте про те, щоб скористатися можливостями непередбачуваності щодо агресора (див. «Комунікацію» нижче).

б) Можливості:

- Розробіть інструменти, методи та процедури для виявлення більш широкого спектру потенційних гібридних загроз, з більшою впевненістю, ніж раніше.

- Розширте спектр інструментів, доступних як для усунення вразливостей, так і для переслідування заходів стримування, спрямованих назустріч агресору, використовуючи як вертикальну, так і горизонтальну ескалацію.

- Розробіть механізми координації та культуру, необхідні для комплексного, загальноурядового та багатонаціонального підходу до політики гібридного стримування.

в) Комунікація - встановіть чіткі та реалістичні порогові значення для стримування та реагування. Занадто низькі вони будуть неспроможними і потенційно контрпродуктивними (не всі гібридні загрози можуть бути стримуваними в усі часи), а поставлені занадто високо – вони можуть спонукати до агресії. Визначення порогів спрямовано проти конструктивної двозначності. Добре позначені пороги допоможуть уникнути прорахунків, але знання «червоних ліній» може спонукати агресію трохи нижче них. Приховані або розпливчасті пороги можуть стримуватися через непередбачуваність, але також можуть спричинити прорахунок. Майте на увазі, що всі дії комусь щось повідомляють. Ключем до успішних стратегічних комунікацій є розуміння аудиторії, розуміння та використання інформаційного середовища, а також інтеграція слів та дій у загально урядовій діяльності.

3) Відповісти. Цей компонент розглядає, як реагувати на гібридні загрози чи атаки, і пропонує основу для цього. Рішення про реагування шляхом впровадження відповідних дій та заходів може бути прийняте на будь-якому етапі циклу гібридної загрози, від виявлення потенційних вразливостей, що вимагають активності зі зміцнення стійкості, до каральних заходів, вжитих у відповідь на гібридну атаку.

На основі отриманих результатів потрібно розробити інституційний механізм реалізації цих заходів через національні уряди та багатонаціональні інституції, щоб переконатися, що він відповідає цілям. «Інституційний механізм» – процеси, механізми, люди та навички – це те, що необхідно для протидії гібридній війні. Він ґрунтується на тому, що [72]:

- протидія гібридній війні є «загально урядовою» діяльністю;
- протидія гібридній війні вимагає багатонаціонального підходу;
- замість того, щоб створювати нові інституційні механізми, існуючі інститути, процеси та організації повинні бути скориговані та доповнені.

6.4. Принципи побудови механізмів захисту від гібридних загроз

Концепція стійкості набуває дедалі більшої актуальності в дискурсі як ЄС, так і НАТО за останні двадцять років. Більше того, за останні п'ять років ЄС і НАТО дедалі більше пов'язують стійкість з боротьбою проти гібридних загроз і підходять до цієї концепції з більш цілісної перспективи. Водночас гібридні загрози відіграють дедалі важливішу роль в політиці ЄС протягом останнього десятиліття, оскільки безпекове середовище ЄС кардинально змінилося, і

Євросоюз відповідно змушений адаптуватися. В нових базових документах ЄС і НАТО стійкість описується як найважливіший елемент запобігання гібридним загрозам і захисту від них. Наразі ми спостерігаємо стрімкий розвиток подій і зростання витонченості гібридних загроз. Тому стійкість до гібридних загроз необхідно розробляти і впроваджувати на всіх рівнях, а також розглядати показники стійкості не лише з точки зору різних сфер, але й як комплексний екосистемний підхід. Іншими словами, розвиток стійкості до гібридних загроз вимагає виходу за межі стійкості в окремих сферах, розбудовуючи її системно, враховуючи залежності та взаємозалежності між різними частинами суспільства – шляхом розбудови комплексної екосистеми стійкості [73], яка має полегшити процес прийняття обґрунтованих управлінських рішень на різних рівнях управління.

«Модель комплексної екосистеми стійкості» («The comprehensive resilience ecosystem (CORE) model») - це системне представлення демократичного суспільства в цілому. Вона використовується для аналізу і, зрештою, протидії гібридним загрозам, які прагнуть підірвати і завдати шкоди цілісності та функціонуванню демократій, змінити процеси прийняття рішень і створити каскадні ефекти [73].

Новизна цієї моделі полягає в тому, що вона дозволяє політикам оцінити, як супротивники використовують гібридні загрози, щоб змінити можливості демократичного прийняття рішень. Вона показує, як гібридні загрози крок за кроком кидають виклик демократичним системам, створюючи різні види стресу. Це також дозволяє відстежувати залежності та можливі каскадні ефекти. Це важливо для виявлення гібридних загроз. Передбачення відіграє вирішальну роль у цьому процесі.

«Модель комплексної екосистеми стійкості» базується на наступних елементах [73]:

а) В основі екосистеми лежать сім засад демократичних систем:

1. відчуття справедливості та рівного ставлення,
2. громадянські права і свободи,
3. політична відповідальність та підзвітність,
4. верховенство права,
5. стабільність,
6. надійність/доступність,
7. здатність до передбачення.

Ці сім засад є основою стійкого, демократичного суспільства і є важливими для розбудови стійкості до гібридних загроз. Саме вони є кінцевими цілями атак ворожих акторів для задоволення при цьому їхніх власних стратегічних інтересів.

б) Домени (сфери) з «Концептуальної моделі гібридних загроз» [8] також є невід'ємною частиною екосистеми: інфраструктурна, кібернетична, космічна, економічна, військова/оборонна, культурна, соціальна/суспільна сфери, сфера

державного управління, правова, розвідувальна, дипломатична, політична, інформаційна сфери. Якщо в доменах добре розвинена стійкість, вони можуть діяти як щити проти зловмисних дій. З іншого боку, відсутність стійкості в доменах може відкрити точки входу для ворожих акторів.

в) Екосистема складається з трьох просторів – Громадянського простору, Простору управління та Простору послуг, які представляють три сектори суспільства.

г) Три рівні екосистеми представляють різні «шари», які існують в організації суспільства – локальний, національний, міжнародний.

Зв'язки між чотирма типами елементів представляють підхід, що охоплює все суспільство (табл. 6.4).

Таблиця 6.4

Схематична візуалізація взаємозв'язків елементів «Моделі комплексної екосистеми стійкості»

Простори	Засади демократичних систем	Домени (сфери)	Рівні		
			Локальний	Національний	Міжнародний
Громадянський простір	1. відчуття справедливості та рівного ставлення, 2. громадянські права і свободи, 3. політична відповідальність та підзвітність,	культурна, соціальна/суспільна сфера, політична сфера, інформаційна сфера	Громади	Нації	Групи та мережі
Простір управління	4. верховенство права, 5. стабільність,	військова/оборонна сфера, сфера державного управління, правова сфера, розвідувальна сфера, дипломатична сфера, політична сфера	Місцевий рівень управління	Управління на державному рівні	Багатосторонній рівень управління
Простір послуг	6. надійність/доступність, 7. здатність до передбачення.	Інфраструктурна сфера, кібернетична сфера, космічна сфера, економічна сфера, інформаційна сфера	Кластерний рівень у сфері послуг	З'єднання	Глобальний рівень у сфері послуг

Джерело: сформовано на основі [73]

Оскільки елементи взаємопов'язані, заходи з розбудови стійкості з для одного елемента впливатимуть на інші елементи, позитивно чи негативно. Актори, що стоять за гібридними загрозами, прагнуть використати різні

елементи та їхній взаємозв'язок для максимізації свого впливу. Тому політикам необхідно розуміти взаємозалежність між різними елементами, щоб розбудовувати стійкість до гібридних загроз і своєчасно виявляти зловмисну діяльність на ранніх стадіях.

Такий екосистемний підхід допомагає виявити ранні сигнали, підтримувати їхній аналіз та визначати потенційні траєкторії реагування. «Модель комплексної екосистеми стійкості» можна використовувати як «дошку для гри в Дартс» для відображення того, як актори використовують конкретні інструменти для атак на різні сфери і створюють каскадні ефекти в різних просторах і на різних рівнях. Це допомагає проаналізувати і зрозуміти вплив, розвиток/етапи, а також те, наскільки інтенсивно, на які сфери і рівні впливають гібридні загрози і наскільки вони залежать одне від одного. По суті, це допомагає особам, які приймають рішення, вибрати, які ресурси, інструменти і заходи мобілізувати на рівні ЄС, держав-членів і на оперативному рівні.

Стійкість є ключем до протидії гібридним загрозам і має розроблятися системно. Розбудова стійкості в окремих сферах окремо не є оптимальним, оскільки гібридні загрози мають на меті створювати каскадні ефекти та використовувати взаємозв'язки. Необхідний системний підхід, з урахуванням існуючих залежностей та взаємозалежностей в суспільстві.

Світове середовище безпеки змінилося, і стає очевидним, що демократичні системи опинилися під загрозою. Гібридні загрози стали невід'ємною частиною світової безпеки. Незважаючи на те, що такі загрози займають важливе місце в політичному порядку денному, розуміння їх різними зацікавленими сторонами (державами, інституціями та іншими відповідними акторами) значно відрізняється.

Гібридні загрози часто називають «злісними проблемами» (Wicked problem) із-за того, що такі проблеми складно або неможливо вирішити внаслідок неповноти, суперечності або мінливості інформації і вхідних умов [74].

Такі проблеми легко стають мішенню гібридних зловмисників, бо злісні проблеми неможливо вирішити. Прийняття рішень у цій площині не буває легким та вимагає міцної системи цінностей, вміння знайти потрібну інформацію та побачити повну картину, розуміння поняття «справедливість» та моральної готовності обирати краще з поганих рішень. Рішення злісних проблем завжди міститиме негативні наслідки. Але, на відміну від маніпуляцій, стійкість особи, що приймає рішення має проявлятись в наступному [3]:

- пильність: вміння знаходити та обирати джерела інформації з вимогами до достовірності (підтвердження об'єктивності даних), надійності (підтвердження інформації з кількох джерел), авторитетності (підтвердження експертності джерела) та актуальності (своєчасності);
- свідомий вибір: вміння формувати та зважувати аргументи;
- стійкість: спроможність приймати ефективні обґрунтовані рішення навіть під впливом негативних чинників.

КОНТРОЛЬНІ ПИТАННЯ

1. Охарактеризуйте документи ЄС щодо ідентифікації та протидії гібридним загрозам.
2. Зазначте хронологію створення організацій, метою діяльності яких є проведення досліджень з питань генезису та трансформування гібридних загроз.
3. Охарактеризуйте Концепцію комплексної безпеки (на прикладі фінської моделі).
4. Охарактеризуйте «Систему протидії гібридній війні».
5. Охарактеризуйте «Модель комплексної екосистеми стійкості».

ТЕСТИ

1. Фінська модель готовності, в якій влада, бізнес, неурядові організації та громадяни несуть спільну відповідальність за захист життєдіяльності суспільства, називається:
а) Концепція комплексної безпеки;
б) Система протидії гібридній війні;
в) Модель комплексної екосистеми стійкості;
г) Концептуальна модель гібридних загроз.
2. Вкажіть, що з переліченого є ключовим елементом забезпечення життєво важливих функцій, відповідно до Концепції комплексної безпеки:
а) готовність;
б) стійкість;
в) екосистема;
г) обороноздатність.
3. Оберіть «три кити» стримування відповідно до «Системи протидії гібридній війні»:
а) Довіра, Можливості, Комунікація;
б) Економіка, Інфраструктура та Безпека постачання;
в) Міжнародна діяльність, Діяльність в ЄС, Внутрішня безпека;
г) Лідерство, Психологічна стійкість, Готовність.
4. Модель, яка використовується для аналізу і, зрештою, протидії гібридним загрозам, які прагнуть підірвати і завдати шкоди цілісності та функціонуванню демократій, змінити процеси прийняття рішень і створити каскадні ефекти, називається:
а) Концепція комплексної безпеки;
б) Система протидії гібридній війні;
в) Модель комплексної екосистеми стійкості;
г) Концептуальна модель гібридних загроз.

5. Оберіть на яких елементах базується «Модель комплексної екосистеми стійкості»:

а) сім засад демократичних систем;

б) три рівні екосистеми представляють різні «шари», які існують в організації суспільства – локальний, національний, міжнародний;

в) з трьох просторів – Громадянського простору, Простору управління та Простору послуг, які представляють три сектори суспільства;

г) всі відповіді вірні.

ТЕРМІНОЛОГІЧНИЙ СЛОВНИК

«Аналітична модель для розуміння гібридної війни», що фокусується на вразливих місцях захисника, здатності нападника в гібридній війні синхронізувати широкий спектр своїх можливостей під час атаки, а також на ефектах, створених в результаті цих дій проти конкретних вразливостей його наміченої цілі [14].

Гібридна війна передбачає синхронізоване використання багатьох інструментів впливу, підібраних з урахуванням конкретних вразливостей у всьому спектрі соціальних функцій для досягнення синергетичних ефектів [14].

Гібридна загроза – скоординована та синхронізована дія, яка свідомо спрямована на системні вразливості демократичних держав та інститутів за допомогою широкого спектру засобів [17].

Європейський центр передового досвіду з протидії гібридним загрозам (The European Centre of Excellence for Countering Hybrid Threats - Hybrid CoE), метою функціонування якого є протидія «новим загрозам, спрямованим на дестабілізацію ситуації в європейських країнах». Діяльність Hybrid CoE спрямована на: проведення досліджень, аналіз гібридних загроз та методів боротьби з ними; організацію спільного навчання для країн-учасниць; проведення консультацій на стратегічному рівні між учасниками ЄС та НАТО, залучення до діалогу урядових та неурядових експертів [32].

«Концептуальна модель гібридних загроз» («Hybrid Threats conceptual model») охоплює ключові елементи, які формують ландшафт гібридних загроз: актори, які застосовують гібридні механізми, фази гібридної кампанії, інструменти та цільові домени (сфери) для досягнення стратегічних цілей ворожого актора [8].

Концепція комплексної безпеки – це фінська модель готовності, в якій влада, бізнес, неурядові організації та громадяни несуть спільну відповідальність за захист життєдіяльності суспільства [69].

«Модель комплексної екосистеми стійкості» («The comprehensive resilience ecosystem (CORE) model») - це системне представлення демократичного суспільства в цілому. Вона використовується для аналізу і, зрештою, протидії гібридним загрозам, які прагнуть підірвати і завдати шкоди цілісності та функціонуванню демократій, змінити процеси прийняття рішень і створити каскадні ефекти [73].

Об'єднаний дослідницький центр Європейської комісії (Joint Research Centre - JRC) надає незалежні, науково обґрунтовані знання, підтримуючи політику ЄС з метою позитивного впливу на суспільство [31].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Місюра А.О., Паливода В.О. Концептуальні підходи НАТО та ЄС до забезпечення стійкості держави і суспільства у сфері національної безпеки: Аналітична записка. ULR: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/konceptualni-pidkhodi-nato-ta-es-do-zabezpechennya-stiykosti

2. Резнікова О.О. Національна стійкість в умовах мінливого безпекового середовища: монографія. Київ: НІСД, 2022. 532 с. ULR: https://niss.gov.ua/sites/default/files/2022-03/reznikova-ukraineresilience2022_02.pdf

3. Методика навчання в умовах гібридних загроз: посібник / Е. Балашов, М. Білоконь, Т. Борозенцева, М. Головянко, С. Гришко, Т. Жовтенко та ін. Харків: ТОВ «ТЕХНО-ЛОГІЧНИЙ ЦЕНТР ГРУП», 2023. 84 с. ULR: https://sciencebookgroup.org/catalog/book/338

4. Карпенко Ю.В., Кобзар А.С. Основні підходи до визначення сутності поняття «управлінське рішення». *Науковий вісник Одеського національного економічного університету*. DOI:10.32680/2409-9260-2021-11-12-288-289-147-153. ULR: http://n-visnik.oneu.edu.ua/collections/2021/288-289/pdf/147-153.pdf

5. Пушкар З., Пушкар Б. Сутність та роль управлінських рішень в управлінні персоналом. ULR: http://dspace.wunu.edu.ua/bitstream/316497/3274/1/%D0%9F%D1%83%D1%88%D0%BA%D0%B0%D1%80%20%D0%97..pdf

6. Євтушенко О.Н. Управлінські рішення: сутність та характерні риси. *Наукові праці. Державне управління*. Вип. 237. 2014. С. 47-51.

7. Хопкінс Дж. (2021). Протидія когнітивній війні: інформованість і стійкість. NATO REVIEW. ULR: https://www.nato.int/docu/review/uk/articles/2021/05/20/protidya-kogntivnj-vjn-nformovanst-stjkst/index.html

8. Cullen, P., Juola, C., Karagiannis, G., Kivisoo, K., Normark, M., Rácz, A., Schmid, J. and Schroefl, J., The landscape of Hybrid Threats: A Conceptual Model (Public Version), Giannopoulos, G., Smith, H. and Theocharidou, M. editor(s), EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305. URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC123305

9. Гібридна війна проти держави: історія, інструменти, технології. ULR: https://sidcon.com.ua/tpost/x3gk5zm1d1-gbridna-vina-proti-derzhavi-storya-nstru

10. Kaldor, M. Human Security: Practical Possibilities. *LSE Public Policy Review*. 2020. 1(2), P. 7. DOI: http://doi.org/10.31389/lseppr.15

11. Hoffman, F., Mattis, James N. Future Warfare: The Rise of Hybrid Wars. USMCR(Ret.), 2005. URL: http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf

12. Schmid, Johann. Der Archetypus hybrider Kriegführung. Hybride Kriegführung vs. Militärisch zentrierte Kriegführung. In: *Österreichische Militärische Zeitschrift (ÖMZ)*, 2020. Heft 5/2020, P. 570–579.

13. Рева Т. Гібридні загрози та гібридні війни: сутність та аспекти взаємодії. *Вісник Львівського університету. Серія філос.-політолог. студії*. 2022. Випуск 40, с. 186–191. DOI https://doi.org/10.30970/PPS.2022.40.24.

14. Cullen, Patrick J, Reichborn-Kjennerud, Erik. MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare A Multinational Capability Development Campaign project (2017). 36 p. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

15. Glossary Hybrid Threats / Глосарій з гібридних загроз / упоряд. С.В.Гришко та ін.; за заг. ред. С.В. Гришко. 2021. 113 с. URL: https://openarchive.nure.ua/handle/document/16258.

16. WARN Project Website. URL: http://warn-erasmus.eu

17. Hybrid threats as a concept. Hybrid CoE. ULR: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

18. Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K., & McCue, M. (2018). Addressing hybrid threats. Swedish Defence University. 93 p. ISBN 978-91-86137-73-1. ULR: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Treverton-AddressingHybridThreats.pdf

19. Pawlak, P. (2017). Countering hybrid threats: EU-NATO cooperation. European Parliamentary Research Service. 12 p. https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf

20. The World Hybrid War: Ukrainian Forefront: monograph abridged and translated from ukrainian / Volodymyr Horbulin. Kharkiv: Folio, 2017. 158 p.

21. Joint Communication to the European Parliament and the Council «Joint Framework on countering hybrid threats the European Union response». 2016. URL: https://eur-lex.europa. eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.

22. Sadık, Giray. Introduction: Hybrid Threats and European Security. Europe's Hybrid Threats: What Kinds of Power Does the EU Need in the 21st Century? Cambridge Scholars Publishing, 2017. P. 1–11.

23. Wigell, Mikael. Hybrid interference as a wedge strategy: a theory of external interference in liberal democracy. *International Affairs*, Volume 95, Issue 2, March 2019, P. 255–275.

24. Томашевський С. Комплексний аналіз оперативної обстановки (PMESII-АНАЛІЗ) Рекомендації та кращі кейси реалізації стратегічних комунікацій в умовах війни: практичний довідник / [В. Азарова та ін. ; за заг. ред. Л. Компанцевої]. Київ : 7БЦ, 2023. С. 90-92.

25. Challenging the application of pmesii-pt in a complex environment by MAJ Brian M. Ducote, SVC, 102 p. ULR: https://apps.dtic.mil/sti/tr/pdf/ADA523040.pdf

26. Методичний посібник для військ (сил) з питань цивільно-військового співробітництва Під загальним керівництвом полковника О.Ноздрачова. Управління цивільно-військового співробітництва Збройних Сил України, 2019. ULR: https://sprotyvg7.com.ua/wp-content/uploads/2022/04/Методичний-посібник-для-військ-з-питань-цивільно-військового-співробітництва.pdf

27. Muhammad, Mudassar Yamin, Mohib, Ullah, Habib, Ullah, Basel, Katt Weaponized AI for Cyber Attacks. ULR: https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/3021130/Weaponized_AI_for_Cyber_Attacks__2_.pdf?sequence=1

28. Burton, J., Soare, S. R. (2019). Understanding the Strategic Implications of the Weaponization of Artificial Intelligence. In T. Minarik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, & G. Visky (Eds.), 2019 11th International Conference on Cyber Conflict: Silent Battle, CyCon 2019 (pp. 1-17). Article 8756866 (International Conference on Cyber Conflict, CYCON; Vol. 2019-May). NATO CCDCOE. https://doi.org/10.23919/CYCON.2019.8756866

29. Бостром Нік. Суперінтелект. Стратегії і небезпеки розвитку розумних машин / пер. з англ. Антон Ящук, Антоніна Ящук. Київ:Наш формат, 2020. 408 с.

30. Козловець М. Технології штучного інтелекту та їх вплив на буттєвість людини *Humanities Studies.* 2024. Випуск 19 (96). URL: http://humstudies.com.ua/article/view/307056

31. Joint Research Centre. URL: https://commission.europa.eu/about-european-commission/departments-and-executive-agencies-old/joint-research-centre_en

32. The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). URL: https://www.hybridcoe.fi/about-us/

33. Семенчук Т.Б., Боняр С.М., Осипова Є.Л. та ін. Менеджмент креативних індустрій: навчальний посібник. Київ: ДУІТ, 2024. 330 с.

34. Council of the European Union. 2008. «Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection». *Official Journal of the European Union*, 75–82.

35. Defense Intelligence Agency. 2019. Challenges to Security in Space.

36. Blackwill, R. D., Harris, J. M. 2016. The Lost Art of Economic Statecraft. *Foreign Affairs 95 (2):* 99–110.

37. Iancu, Niculae, Andrei Fortuna, Cristian Barna, and Mihaela Teodor. 2016. Countering Hybrid Threats: Lessons Learned from Ukraine. Washington: IOS Press.

38. Fabre, Cécile. 2018. Economic Statecraft: Human Rights, Sanctions, and Conditionality. Cambridge: Harvard University Press.

39. Norris, William J. 2016. Chinese Economic Statecraft: Commercial Actors, Grand Strategy, and State Control. Ithaca: Cornell University Press.

40. Giles, Keir, Philip Hanson, Roderic Lyne, James Nixey, James Sherr, and Andrew Wood. 2015. The Russian Challenge, Chatham House Report. London: Chatham House, the Royal Institute of International Affairs

41. Wilson, Jeanne L. 2016. Cultural Statecraft in the Russian and Chinese Contexts: Domestic and International Implications. *Problems of PostCommunism.* 63 (3): 135–45. https://doi.org/10.1080/10758216.2015.1132630

42. Kettl, Donald F. 2018. Politics of the Administrative Process. 7th ed. Los Angeles: CQ Press.

43. Savolainen, J. 2018. Legal Resilience Workshop, Helsinki, Finland. European Centre of Excellence for Countering Hybrid Threats.

44. Lowenthal, Mark M. 2015. Intelligence: From Secrets to Policy. 6th ed.

45. Wallace, Helen, Mark A Pollack, and Alasdair R Young. 2015. Policy-Making in the European Union. 7th ed. Oxford: Oxford University Press.

46. Viotti P.R., Kauppi P.R. 2012. International Relations Theory. In , 5th ed. New York: Pearson.

47. NATO. 2013. Allied Command Operations Comprehensive Operations Planning Directive Interim V2.0. Belgium: North Atlantic Treaty Organization, Supreme Headquarters Allied Powers Europe.

48. Putnam, R D. 1988. Diplomacy and Domestic Politics: The Logic of Two-Level Games. International Organization 42 (3): 427–60.

49. European Convention for the Protection of Human Rights and Fundamental Freedoms, Article 10. URL: https://www.echr.coe.int/Documents/Convention_ENG.pdf

50. Heal, Sid. 2008. Shaping Operations. The Tactical Edge.

51. Molden, Daniel C. 2014. Understanding Priming Effects in Social Psychology: What Is «Social Priming» and How Does It Occur? *Social Cognition*. Vol. 32.

52. Mattlin, Mikael, Nojonen, Matti. 2011. Conditionality in Chinese Bilateral Lending. In BOFIT Discussion Papers, edited by Laura Solanko. Bank of Finland.

53. Moyer, Jonathan D, Tim, Sweijs, Mathew, J Burrows, and Hugo, Van Manen, eds. 2018. Power and Influence in a Globalized World. *Atlantic Council*.

54. Schmid, Johann. 2019. The Hybrid Face of Warfare in the 21st Century. *Maanpuolustus.*

55. Pindják, Peter. 2014. Deterring Hybrid Warfare: A Chance for NATO and the EU to Work Together? *NATO Review*.

56. Clausewitz, Carl. 1976. On War (Edited and Translated by Michael Howard, Peter Paret). Princeton: Princeton University Press,.

57. Arreguín-Toft, Ivan. 2001. How the Weak Win Wars: A Theory of Asymmetric Conflict. International Security 26 (1): 93–128. https://doi.org/10.1162/0162288017532128 68

58. Habermayer, Helmut. 2011. Hybrid Threats and a Possible Counter-Strategy. In Hybrid and Cyber War as Consequences of the Asymmetry, edited by Josef Schröfl, Bahram M Rajaee, and Dieter Muhr, 249–72. New york: Peter Lang.

59. Countering hybrid threats: EU-NATO cooperation. URL: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2017)599315

60. Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats — a European Union response/European Commission. . URL: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

61. Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign And Security Policy. URL: https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf

62. Joint Report to the European Parliament and the Council on the implementation of the Joint Framework on countering hybrid threats — a European Union response/EU Council. URL: http://data.consilium.europa.eu/doc/document/ST-11539-2017-INIT/en/pdf

63. Joint Staff Working Document «Eastern Partnership - 20 Deliverables for 2020 Focusing on key priorities and tangible results». URL: https://neighbourhood-enlargement.ec.europa.eu/document/download/a61891ff-e1a9-4118-91cc-4ee7e6b226af_en?filename=EaP%2020%20Deliverables%20for%202020.pdf

64 Countering hybrid threats: EU-NATO cooperation. Briefing/ European Parliamentary Research Service. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf

65. Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization/NATO. . URL: http://www.nato.int/cps/en/natohq/official_texts_133163.htm

66. Гібридні загрози Україні і суспільна безпека. Досвід ЄС і Східного партнерства. Аналітичний документ. За загальною редакцією В.Мартинюка (керівника проекту) Експертна група проекту: М.Гончар, А.Чубик, С.Жук, О.Чижова, Г.Максак, Ю.Тищенко, О.Зварич. Київ : 2018. URL: https://www.civic-synergy.org.ua/wp-content/uploads/2018/04/blok_XXI-end_0202.pdf

67. Міжнародний досвід протидії гібридним загрозам: законодавче регулювання та організації з питань стратегічних комунікацій. URL: http://euinfocenter.rada.gov.ua/uploads/documents/29377.pdf

68. Countering hybrid threats. URL: https://www.nato.int/cps/ru/natohq/topics_156338.htm?selectedLocale=en

69. Turvallisuuskomitea. (2017). *Concept of Comprehensive Security – Building National Resilience in Finland*. URL: https://turvallisuuskomitea.fi/concept-of-comprehensive-security-building-national-resilience-in-finland/

70. The Security Strategy for Society Government Resolution / 2.11.2017. URL: https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf

71. The 72h concept details the level of home preparedness recommended by the authorities and NGOs. URL: https://72tuntia.fi/en/

72. Monaghan, Sean (Ed.), Patrick, Cullen, Wegge, Njord. 2019. MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare." 94 p. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf

73. Jungwirth, R., Smith, H., Willkomm, E., Savolainen, J., Alonso, Villota M., Lebrun, M., Aho, A., Giannopoulos, G., Hybrid threats: a comprehensive resilience ecosystem – Executive summary, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/113791, JRC129019. URL: https://www.hybridcoe.fi/wp-content/uploads/2023/09/JRC129019_02.pdf

74. Cullen, P. (2018). Hybrid CoE Strategic Analysis 8: Hybrid threats as a new «wicked problem» for early warning. Hybrid CoE. URL: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-Analysis-2018-8-Cullen.pdf

Co-funded by the
Erasmus+ Programme
of the European Union

ГІБРИДНІ ЗАГРОЗИ ТА КОМПЛЕКСНА БЕЗПЕКА

Навчальний посібник
для здобувачів другого (магістерського)
рівня вищої освіти

Підп. до друку 05.07.2024. Формат вид. 60х80 1/16
Папір офсет. № 1. Офс. друк. Гарн. «Times New Roman Cyr»
Ум. друк. арк. 4,51. Обл.-вид.арк. 4,28.
Наклад 300 прим. Зам. 157

Віддруковано в типографії
ТОВ «ТРОПЕА»,
м. Київ, 2024