МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н. Каразіна

Навчально-науковий інститут «Інститут державного управління»
Кафедра права, національної безпеки та європейської інтеграції

Кваліфікаційна робота магістра
на тему

ВИКОРИСТАННЯ МІЖНАРОДНОГО ДОСВІДУ У СФЕРІ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ ДЛЯ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ

Виконав студент 2 курсу,
групи ППГЗ-2-24
Спеціальності 281 «Публічне управління та адміністрування»
Освітньо-професійної програми
«Публічна політика та управління в умовах гібридних загроз»
_____ Юрій ГРИСЬКОВ

Науковий керівник роботи:
кандидат наук з державного управління, доцент
_____ Михайло БІЛОКОНЬ

Харків – 2025

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

ГУР	Головне управління розвідки
ЄС	Європейський Союз
ЗСУ	Збройні Сили України
КМУ	Кабінет Міністрів України
МЗС	Міністерство закордонних справ
МКІП	Міністерство культури та інформаційної політики
МОУ	Міністерство оборони України
НАТО	Організація Північноатлантичного договору
НУО	Неурядова/Недержавна організація
ПУОП	Психологічні операції
РНБО	Рада національної безпеки і оборони
СБУ	Служба безпеки України
ССО	Сили спеціальних операцій
СтратКом	Стратегічні комунікації
ЦПД	Центр протидії дезінформації
ЦСКІБ	Центр стратегічних комунікацій та інформаційної безпеки
AJP-10	Allied Joint Doctrine for Strategic Communications (Об'єднана союзна доктрина зі стратегічних комунікацій)
ARW	Advanced Research Workshop (Семінар НАТО з поглиблених досліджень)
COLMI	Оперативний комітет з протидії інформаційним маніпуляціям (Франція)
DSB	Defense Science Board (Рада з питань оборонної науки США)
EEAS	European External Action Service (Європейська служба зовнішніх справ)
ELM	Elaboration Likelihood Model (Модель ймовірності обробки інформації)
ESTF	East Stratcom Task Force (Східна робоча група зі СтратКом)

FIMI	Foreign Information Manipulation and Interference (Маніпулювання зовнішньою інформацією та втручання)
GCS	Government Communication Service (Урядова служба комунікацій, Велика Британія)
Hybrid CoE	European Centre of Excellence for Countering Hybrid Threats (Європейський центр передового досвіду з протидії гібридним загрозам)
Info Ops	Information Operations (Інформаційні операції)
JRC	Joint Research Commission (Спільна дослідницька комісія ЄС)
M&E	Monitoring and Evaluation (Моніторинг та Оцінка)
MCOM	Modern Communications Operating Model (Сучасна операційна модель комунікацій)
MENA	Middle East and North Africa (Близький Схід та Північна Африка)
MilPA	Military Public Affairs (Військові зв'язки з громадськістю)
PA	Public Affairs (Зв'язки з громадськістю)
PD	Public Diplomacy (Публічна дипломатія)
PSYOP	Psychological Operations (Психологічні операції)
RAS	Rapid Alert System (Система швидкого сповіщення ЄС)
RRN	Reliable Recent News (Операція FIMI «Doppelgänger»)
SIG	Service d'information du Gouvernement (Служба інформації Уряду, Франція)
StratCom COE	Strategic Communications Centre of Excellence (Центр передового досвіду НАТО зі стратегічних комунікацій)
TFS	Task Force South (Робоча група Півдня, ЄС)
USIA	United States Information Agency (Інформаційне агентство США)
VIGINUM	(Французька) агенція з онлайн-розслідувань
WBTF	Western Balkans Task Force (Робоча група по Західних Балканах, ЄС)

ВСТУП

Актуальність даного дослідження зумовлена фундаментальною трансформацією безпекового середовища, в якому опинилася сучасна держава. Класична дихотомія «мир-війна» поступилася місцем стану «перманентної конфронтації», що ведеться переважно у так званій «сірій зоні». Цей новий тип конфлікту – гібридна війна – становить пряму загрозу не стільки військовій силі, скільки самій системі публічного управління та адміністрування.

Проблема полягає в тому, що гібридні загрози за своєю суттю є координованим використанням системних вразливостей відкритого суспільства. Сильні сторони ліберальної демократії – вільна преса, верховенство права, економічна відкритість – цілеспрямовано перетворюються агресором на головні вразливості. Кінцевою метою таких атак є не фізичне завоювання, а параліч державних інститутів, підрив довіри до влади та блокування процесів прийняття рішень. Таким чином, сфера публічного управління та адміністрування перетворюється з механізму забезпечення державної політики на головне поле бою гібридної війни.

Критичний аналіз відомих підходів до розв’язання цієї проблеми виявляє небезпечний стратегічний дисбаланс. Сучасна практика протидії, як в Україні, так і в багатьох країнах-партнерах, демонструє стратегічний перекіс у бік «оборони» (реактивності). Переважна більшість зусиль та ресурсів спрямована на захисні функції: спростування фейків, підвищення медіаграмотності та розбудову суспільної «стійкості».

Хоча ці заходи є життєво важливими, дослідження (зокрема, звіти Hybrid CoE) показують, що надмірна залежність від стійкості є «пасткою». Ця пасивна, оборонна модель:

– Прирікає державу на реактивність: Система змушена постійно «наздоганяти» ворога, реагуючи на ті наративи, які він нав'язує, замість того, щоб просувати власний порядок денний.

– Створює стратегічну асиметрію: Агресор, не стикаючись із реальними наслідками своїх дій, може безкарно та з низькими витратами генерувати нескінченний потік атак. Надмірна опора на стійкість, по суті, «запрошує до експлуатації».

– Ігнорує «накладення витрат»: У поточному підході практично відсутній інституціоналізований компонент «меча» – проактивних, наступальних дій, що карали б джерела загроз, а не лише боролися з їхніми наслідками.

Доцільність роботи для галузі публічного управління та адміністрування полягає у вирішенні цієї фундаментальної проблеми. Сучасна українська система характеризується інституційною фрагментацією та відсутністю єдиного координаційного центру, що призводить до «розсинхронізації» дій влади і робить державний апарат неефективним перед обличчям скоординованих гібридних атак.

Таким чином, актуальність дослідження полягає у науково-практичній потребі вийти за межі реактивної моделі «стійкості» та обґрунтувати нову модель державної політики у цій сфері. Шляхом аналізу та адаптації міжнародного досвіду (США, Великої Британії, Франції, ФРН, НАТО та ЄС) дана робота пропонує конкретні інституційні рішення для побудови в Україні збалансованої, «гібридної» системи стратегічних комунікацій. Ця система має поєднувати централізовану координацію (за французькою моделлю), вимірювання ефективності (за британською) та проактивний компонент «накладення витрат» (за американською та моделлю НАТО).

Розробка такої ефективної, проактивної та інституційно злагодженої системи є одним із ключових завдань сучасного публічного управління та умовою збереження суверенітету держави в умовах гібридної війни.

Мета даної магістерської роботи полягає в тому, щоб на основі аналізу міжнародного досвіду у сфері стратегічних комунікацій розробити науково обґрунтовані рекомендації щодо вдосконалення державної політики України та посилення інституційної спроможності національної системи протидії

гібридним загрозам.

Для досягнення поставленої мети в роботі визначено такі *завдання*:

– З'ясувати еволюцію та сутність понять «гібридна війна» та «гібридні загрози», проаналізувавши їх трансформацію від тактичних концепцій до стратегічного інструменту впливу на когнітивну сферу та процеси прийняття рішень.

– Проаналізувати теоретичні (психологічні, комунікаційні) основи та простежити історичний (доктринальний) розвиток стратегічних комунікацій як інструменту державної політики у сфері безпеки та оборони.

– Систематизувати та охарактеризувати ключові правові та інституційні механізми стратегічних комунікацій, що застосовуються у провідних країнах світу та міжнародних безпекових організаціях (НАТО, ЄС).

– Узагальнити успішні практики та «засвоєні уроки» міжнародного досвіду з протидії складним гібридним інформаційно-психологічним впливам.

– Виявити фундаментальні прогалини в поточній українській системі публічного управління у сфері СтратКом (зокрема, інституційну фрагментацію та «пастку стійкості») та визначити можливості для адаптації релевантного міжнародного досвіду.

– Обґрунтувати пріоритетні напрями та надати практичні рекомендації щодо посилення інституційної спроможності та ефективності національної системи стратегічних комунікацій шляхом її реформування та впровадження збалансованої «гібридної» моделі.

Об'єктом дослідження є процес формування та реалізації державної політики у сфері стратегічних комунікацій, спрямованої на протидію гібридним загрозам.

Предметом дослідження є використання міжнародного досвіду у сфері стратегічних комунікацій для протидії гібридним загрозам.

Методи дослідження. Для досягнення поставленої мети та розв'язання визначених завдань у магістерській роботі було використано комплекс загальнонаукових та спеціальних методів дослідження, що становлять

методологічне підґрунтя сучасної науки про публічне управління та адміністрування.

Загальнонаукові методи:

– Аналіз та синтез – застосовувалися для деконструкції складних понять «гібридна війна» та «стратегічні комунікації» на окремі елементи, а також для синтезування цілісних висновків та рекомендацій.

– Історико-логічний метод – дозволив простежити еволюцію доктрин СтратКом від часів Холодної війни до сучасності, виявивши ключові каталізатори змін (наприклад, атаки 9/11 та агресія рф 2014 року).

– Систематизація та класифікація – використані для структурування та групування різних національних та інституційних моделей стратегічних комунікацій (НАТО, ЄС, США, ФРН, Франція, Велика Британія).

Спеціальні методи:

– Порівняльний (компаративний) аналіз – виступив ключовим методом дослідження, що дозволив зіставити сильні та слабкі сторони правових та інституційних підходів різних держав та організацій до протидії гібридним загрозам.

– Інституційний аналіз – застосовувався для вивчення повноважень, функцій та взаємозв’язків ключових державних органів у сфері СтратКом.

– Аналіз документів – став основою для опрацювання доктринальних документів, стратегічних концепцій, наукових звітів та нормативно-правових актів.

– Метод моделювання – використаний у третьому розділі для обґрунтування та побудови адаптивної «гібридної» моделі стратегічних комунікацій для України, що включає рекомендації щодо централізації координації та створення «подвійного ядра» («Щит» і «Меч»).

Практичне значення отриманих результатів. Практичне значення магістерської роботи полягає в тому, що її результати та висновки є науково обґрунтованою основою для вдосконалення державної політики України у сфері протидії гібридним загрозам. Отримані результати можуть бути

використані:

– Органами державної влади – зокрема Радою національної безпеки і оборони України, Кабінетом Міністрів України та Апаратом Верховної Ради України – під час реформування та оптимізації національної інституційної системи стратегічних комунікацій, зокрема у процесі уточнення повноважень та координації між Центром протидії дезінформації та Центром стратегічних комунікацій та інформаційної безпеки.

– Безпосередньо у практичній діяльності зазначених центрів (ЦПД та ЦСКІБ) при розробці нових стратегій та планів заходів. Запропоновані рекомендації щодо впровадження «подвійного ядра» («Щит» і «Меч»), переходу до проактивної наративної політики та імплементації системи моніторингу та оцінки за британською моделлю можуть бути покладені в основу оновлення їхніх операційних процедур.

– У навчальному процесі при підготовці магістрів за спеціальностями «Публічне управління та адміністрування» та «Національна безпека», а також у програмах підвищення кваліфікації державних службовців, що працюють у сфері інформаційної безпеки.

– Аналітичними центрами та громадськими організаціями, що працюють у сфері протидії дезінформації, для розробки пропозицій щодо посилення «загальносуспільного» підходу та формалізації співпраці між державним та недержавним сектором.

РОЗДІЛ 1
ТЕОРЕТИКО-ІСТОРИЧНІ ЗАСАДИ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ У СИСТЕМІ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ

1.1 Еволюція та сутність понять «гібридна війна» та «гібридні загрози» в контексті сучасних міжнародних відносин

Сучасні міжнародні відносини характеризуються станом «перманентної конфронтації», що ведеться переважно у когнітивній, інформаційній та економічній сферах. Класична дихотомія «мир-війна» розмилася, поступившись місцем так званій «сірій зоні» [18]. У цьому новому середовищі ревізіоністські державні та недержавні актори [60] кидають виклик встановленому міжнародному порядку, використовуючи гібридні тактики, що цілеспрямовано знаходяться нижче порогу відкритого збройного конфлікту [22]. Ці дії, що включають дезінформацію, кібератаки, економічний примус та використання проксі-сил [60], спрямовані не стільки на фізичне знищення супротивника, скільки на параліч його волі та процесів прийняття рішень.

У той час як концепції «гібридної війни» та «стратегічних комунікацій» (СтратКом) активно вивчаються академічною та військовою спільнотою окремо, існує нагальна потреба в їх глибокому теоретико-історичному синтезі. Необхідно простежити, як еволюція гібридних загроз виступила каталізатором для фундаментальної трансформації стратегічних комунікацій. СтратКом перетворився із набору допоміжних, часто нескоординованих функцій – «білої» публічної дипломатії та «чорних» психологічних операцій [35] – на інтегрований, синхронізований та проактивний інструмент державної політики.

Для проведення аналізу теоретико-історичних засад стратегічних комунікацій як цілісної системи протидії гібридним загрозам потрібно: по-

перше, деконструювати еволюцію поняття «гібридна війна», від початкової концепції Френка Хоффмана [23] до сучасного розуміння, що базується на стратегічній двозначності [28]; по-друге, простежити теоретичний (психологічний, комунікаційний) [25] та історичний (практичний, доктринальний) [35] розвиток СтратКом; по-третє, проаналізувати, як ключові міжнародні (НАТО, ЄС) [22] та національні (Україна) [62] інституції адаптували доктрину СтратКом для нейтралізації специфічних механізмів гібридної війни.

Підйом гібридних загроз, які характеризуються стратегічною двозначністю та системними атаками на когнітивну сферу, виступив головним каталізатором доктринальної трансформації стратегічних комунікацій. СтратКом еволюціонував, перетворившись на інтегровану, синхронізовану функцію державної політики, що є ключем до управління сприйняттям, формування стійких наративів та зміцнення суспільної стійкості – вирішальних факторів для перемоги у «сірій зоні» [18].

Концептуалізація «гібридної війни» у сучасному безпековому дискурсі нерозривно пов'язана з працями Френка Хоффмана, зокрема його монографією «Конфлікт у 21-му столітті: Повстання гібридних війн» (2007) [23]. Ця робота, що стала результатом аналізу нових викликів, з якими зіткнулися західні армії на початку 2000-х років, зокрема в Іраку, Афганістані та під час Другої ліванської війни 2006 року [20], запропонувала новий погляд на характер сучасних конфліктів.

Хоффман, часто у співавторстві з генералом Джеймсом Меттісом, визначив гібридність не як просту наявність нових тактик, а як *синергетичне поєднання* в рамках однієї кампанії різнорідних елементів. Згідно з його визначенням, гібридні загрози гнучко поєднують: 1) конвенційні військові спроможності, 2) іррегулярні тактики (партизанська війна, тероризм, повстанські рухи), 3) інформаційні операції та кібервійну, а також 4) злочинну діяльність для фінансування операцій [23].

Важливим аспектом концепції Хоффмана було розширення суб'єктності.

Він підкреслив, що гібридність притаманна не лише державам, що вдаються до іррегулярних та проксі-методів [19], але й недержавним акторам (наприклад, Хезболла), які отримують доступ до раніше суто державних спроможностей (високоточна зброя, складні системи). Початковий фокус Хоффмана був значною мірою тактичним та операційним: як противники будуть уникати конвенційної переваги США, затягуючи їх у складні асиметричні конфлікти, зокрема у щільній міській забудові [19].

Водночас, стрімка популяризація терміну «гібридна війна» призвела до його семантичної ерозії. Термін швидко перетворився на «модне слівце» («buzzword») [23], що почало втрачати аналітичну чіткість. Як зазначає український дослідник Ю. О. Лобода, надмірне та часто нечітке вживання терміну «гібридна війна» *саме по собі* сприяє поширенню «туману війни». Це створює «когнітивне упередження», відволікаючи увагу суспільства та політиків від «основних рис звичайного збройного конфлікту», який може бути складовою гібридної кампанії [59].

Таким чином, виник парадокс: агресор, що веде гібридну війну, отримує пряму вигоду від того, що об'єкт агресії та міжнародна спільнота починають дискутувати про *семантику* конфлікту («чи є це гібридною війною?», «чи перетнуто поріг?»). Замість того, щоб фіксувати *факт* агресії, час витрачається на дебати, що ускладнює та затримує процес прийняття рішень щодо відповіді. Ця семантична неоднозначність, яку Хоффман розглядав як побічний ефект, у подальших теоріях стала розглядатися як центральний елемент стратегії.

Саме ця еволюція фокусу з тактичного на стратегічний рівень і визначає сучасне розуміння гібридності. Якщо в концепції Хоффмана різні методи (конвенційні, іррегулярні, злочинні) змішувалися для досягнення *військової* переваги на полі бою, то новітні підходи, що часто аналізують доктрину «війни нового покоління», розглядають саму двозначність як основну зброю.

Тут головне поле бою остаточно переноситься з фізичного простору в когнітивний та інформаційний. Агресор цілеспрямовано діє «нижче порогу» чіткої військової відповіді, навмисно розмиваючи межу між станом миру та

станом війни. Це і є та сама «сіра зона», де традиційні механізми міжнародного права та безпекові альянси починають давати збій.

У цій новій парадигмі дезінформація, корупційні впливи, кібератаки на критичну інфраструктуру, енергетичний шантаж та політична дестабілізація перестають бути просто *підтримуючими* заходами. Вони стають *основним інструментом* досягнення стратегічних цілей.

Метою такої кампанії є вже не стільки фізичне знищення армії противника, скільки параліч його державних інститутів, розкол суспільства та руйнування його волі до опору зсередини. Агресор прагне перемогти, так і не давши опоненту чіткого приводу та можливості оголосити війну. Таким чином, семантична плутанина, яку початково вважали побічним ефектом, перетворюється на керований інструмент, що руйнує сам процес прийняття рішень ще до того, як конфлікт переходить у відкриту фазу.

Поворотним моментом у розумінні гібридності стала російська агресія проти України у 2014 році [23]. Поява «зелених чоловічків» у Криму [68] та розпалювання конфлікту на Донбасі змістили аналітичний фокус з *тактичного поєднання* інструментів (за Хоффманом) на *стратегічну мету* цього поєднання.

Британський дослідник Ендрю Мамфорд переосмислив концепцію, запропонувавши тезу, що гібридна війна – це «продовження двозначності іншими засобами» («the continuation of ambiguity by other means») [29]. У його аналізі [28] двозначність (ambiguity) перестає бути побічним ефектом і стає *головним стратегічним інструментом*.

Ключова мета гібридного актора, згідно з цим підходом, – *не* обов'язково повністю приховати свою участь (часто використовується тактика «неправдоподібного заперечення» – «implausible deniability»). Головна мета – «паралізувати легітимну відповідь» («stymie a legitimate response») [28].

Цей параліч досягається через кілька механізмів [28]:

– Дії нижче порогу: Здійснення ворожих дій (наприклад, кібератаки, дезінформація, розгортання сил без розпізнавальних знаків) на рівні, що

знаходиться нижче юридичного та політичного порогу конвенційної військової відповіді [22].

– Створення двозначності: Навмисне створення неясності щодо *походження* (атрибуції), *намірів* та *відповідних заходів у відповідь*.

– Використання «тактики салямі»: Поступова ерозія норм та «відрізання» малих поступок, жодна з яких окремо не виправдовує повномасштабної реакції.

У результаті, держава-жертва та її союзники опиняються перед стратегічною дилемою [28]:

– Надмірна реакція: Якщо відповісти військовою силою на двозначні дії (наприклад, проти «невідомих» «зелених чоловічків»), агресор може звинуватити жертву в ескалації та використати це як привід для відкритого конвенційного вторгнення «з метою захисту».

– Недостатня реакція: Якщо *не* відповідати, очікуючи на повну ясність, це призводить до успіху агресора через «смерть від тисячі порізів».

Таким чином, двозначність – це не просто «туман війни». Це навмисно створений когнітивний параліч, спрямований безпосередньо на цикл прийняття рішень (OODA loop) супротивника. Агресор виграє вирішальний час, поки жертва та її союзники намагаються досягти політичного та юридичного консенсусу щодо *атрибуції* та *характеру* загрози.

Саме в цьому виграному часі й полягає головна стратегічна перевага. Поки держава-жертва та її союзники застрягають у бюрократичних та політичних дебатах, намагаючись «орієнтуватися» та «прийняти рішення», агресор продовжує «діяти». Він швидко створює нову реальність «на землі», закріплюючи свої здобутки.

Коли ж політичний консенсус щодо відповіді нарешті досягається, агресор вже досяг так званого «доконаного факту» (fait accompli). Це фундаментально змінює характер дилеми. Одною справою є запобігти ворожим діям, а зовсім іншою – скасувати вже доконаний результат, наприклад, анексію території. Тепер будь-яка відповідь, спрямована на відновлення попереднього

стану, вимагатиме значно більших зусиль та нестиме незрівнянно вищі ризики повномасштабної ескалації.

Цей когнітивний параліч активно підтримується та посилюється в інформаційній сфері. Агресор цілеспрямовано наповнює глобальний медіапростір суперечливими наративами, теоріями змови та відвертою дезінформацією. Мета цього «інформаційного шуму» – не стільки переконати, скільки остаточно заплутати, посіяти сумнів та унеможливити спільне розуміння реальності. Навіть за наявності чітких доказів розвідки, у публічній площині завжди залишається простір для «альтернативних точок зору», що й надалі гальмує та розколює процес прийняття рішень.

Сучасні гібридні загрози є *координованим* використанням різноманітних заходів [22] для *експлуатації системних вразливостей* відкритого суспільства. Операційний простір, в якому діють ці загрози, отримав назву «сірої зони» (Grey Zone) – стану *між* мирною конкуренцією та відкритим збройним конфліктом [18].

Це простір, який агресор обирає абсолютно свідомо. Він діє в ньому, тому що саме «сіра зона» дозволяє максимально ефективно використовувати переваги відкритих демократичних систем проти них самих.

Наприклад, свобода слова та відкритий медіа-ринок, які є фундаментальними для демократії, стають ідеальними каналами для поширення дезінформації, пропаганди та маніпулятивних наративів. Агресор не повинен пробивати цензуру; він просто використовує існуючі платформи, щоб посіяти сумніви, поглибити суспільний розкол та підірвати довіру до державних інституцій.

Так само, верховенство права та незалежна судова система можуть бути використані для «законного» блокування рішень уряду або для захисту агентів впливу під виглядом дотримання правових процедур. Економічна відкритість дозволяє здійснювати корупційний тиск, купувати стратегічні підприємства або використовувати енергетичні ресурси як інструмент шантажу.

Таким чином, у «сірій зоні» сила демократії – її прозорість, законність та

відкритість – перетворюється на її головну вразливість. Агресор не намагається «зламати» систему ззовні силою, він прагне «роз'їсти» її зсередини, використовуючи її ж власні правила та механізми.

Стратегічна концепція НАТО 2022 року [31] та документи Європейської Комісії [22] чітко вказують, що гібридні загрози експлуатують «відкритість, взаємопов’язаність та цифровізацію» демократичних країн. Це фундаментальний момент: *сильні сторони* ліберальної демократії (вільна преса, відкрита економіка, верховенство права) розглядаються агресором як *вразливості*. Вільна преса вразлива до дезінформації; відкрита економіка – до економічного примусу; верховенство права, що вимагає доказів для атрибуції, – до стратегічної двозначності.

Ця асиметрія в самій природі систем стає ключовим полем бою. Агресор, не обтяжений ані верховенством права, ані необхідністю суспільного консенсусу, може діяти швидко, рішуче та приховано. Натомість демократична держава змушена реагувати повільно. Їй потрібен час на збір беззаперечних доказів, на проведення парламентських слухань, на формування політичної коаліції для ухвалення рішення.

Поки демократія проходить усі ці необхідні, але тривалі процедури, агресор вже закріплює свої здобутки та створює нову реальність «на землі». Таким чином, сам демократичний процес – його прозорість, підзвітність та опора на закон – перетворюється на часову пастку. Агресор використовує нашу процедурну ретельність проти нас, виграючи вирішальний час та ініціативу, поки ми намагаємося дати відповідь, не порушивши власних фундаментальних принципів.

Отже, гібридна війна – це не просто війна *проти* держави; це війна *проти* самої *системи* ліберальної демократії. Її мета – не завоювання території військовим шляхом, а дестабілізація та руйнування системи зсередини через поглиблення поляризації, підрив довіри до демократичних інститутів [17] та параліч інституцій [22].

Ця стратегія, по суті, змушує суспільство атакувати саме себе. Агресор

тут виступає не стільки як прямий загарбник, скільки як модератор внутрішнього хаосу. Він цілеспрямовано «підживлює» вже існуючі в суспільстві розбіжності – політичні, соціальні чи ідеологічні.

За допомогою дезінформації та маніпуляцій у когнітивній сфері, він доводить цю поляризацію до критичної точки, коли конструктивний діалог всередині країни стає неможливим. Коли громадяни втрачають довіру до уряду, до виборчої системи, до судів і навіть один до одного, суспільний договір починає руйнуватися.

В такому стані держава втрачає свою головну опору – внутрішню єдність та здатність до колективних дій. Вона стає «некерованою». І в цей момент агресор досягає своїх цілей, адже такий паралізований та роз'єднаний противник не здатен чинити ефективний опір зовнішньому тиску чи прихованій агресії.

Інструментарій гібридних загроз є багатовимірним і охоплює всі сфери життєдіяльності держави:

– Інформаційно-когнітивний домен: Масові дезінформаційні кампанії [60], маніпулювання політичним наративом у соціальних мережах [22], поширення пропаганди [67] та «зловмисні дії у кіберпросторі» [31].

– Політико-дипломатичний домен: Втручання у демократичні процеси та вибори [31], фінансування радикальних політичних партій та громадських організацій [43], дипломатичний тиск [22].

– Військовий домен: Використання проксі-акторів та нерегулярних формувань, диверсійні операції [60], розгортання сил спеціальних операцій без розпізнавальних знаків [68], а також постійна *загроза* застосування конвенційної сили для підкріплення примусу [31].

– Економічний домен: Широкий спектр економічного тиску [60], включаючи «маніпулювання енергопостачанням» та «економічний примус» [31].

– Соціальний домен: Штучне розпалювання релігійної чи етнічної ворожнечі [43] та «інструменталізація міграції» для створення суспільно-

політичної кризи [31].

Проте, вирішальною характеристикою гібридного підходу є не просто наявність цього широкого арсеналу, а його синхронізоване та інтегроване застосування. Агресор рідко робить ставку на якийсь один інструмент. Навпаки, він діє одночасно в усіх цих сферах, створюючи кумулятивний, або синергетичний, ефект, де кожна дія посилює іншу.

Наприклад, економічний примус, такий як енергетичний шантаж, негайно підтримується в інформаційному просторі. Потужна дезінформаційна кампанія починає пояснювати, що зростання цін чи дефіцит ресурсів є виключно наслідком «некомпетентності» або «недружніх дій» уряду країни-жертви. Водночас, в політичній сфері активізуються фінансовані агресором сили, які вимагають відставки уряду та зміни зовнішнього курсу, використовуючи економічні труднощі як привід.

Таким чином, держава-жертва опиняється під багатовимірним тиском. Їй доводиться одночасно реагувати на економічну кризу, інформаційну атаку та політичну дестабілізацію. Це розсіює її ресурси, паралізує волю до опору та робить практично неможливим вироблення єдиної, узгодженої відповіді.

1.2 Теоретичні основи та історичний розвиток стратегічних комунікацій як інструменту державної політики у сфері безпеки та оборони

Стратегічні комунікації – це значно більше, ніж зв'язки з громадськістю чи інформаційне забезпечення. Це «цілеспрямоване використання комунікації» організацією (державою) для «виконання своєї місії» [45]. Це багатовимірний процес управління комунікацією на всіх рівнях – стратегічному, оперативному та тактичному [43] – для досягнення конкретних і вимірюваних когнітивних та поведінкових ефектів [46]. Щоб зрозуміти, *як* СтратКом працює, необхідно звернутися до його теоретичного ядра, що лежить на перетині соціальної

психології та теорії комунікації.

На мікрорівні (психологія індивіда) СтратКом базується на:

– Управлінні сприйняттям (Perception Management): СтратКом є організаційною формою управління враженнями (Impression Management) [32]. Це «свідома чи несвідома спроба вплинути на сприйняття іншими людьми» держави, її політики чи дій шляхом «регулювання та контролю інформації» [30].

– Теоріях переконання: Для ефективного впливу СтратКом повинен долати фундаментальні психологічні бар'єри. Дослідження вказують на необхідність роботи з «упередженням підтвердження» (confirmation bias) – схильністю людей шукати інформацію, що підтверджує їхні погляди, та «когнітивним дисонансом» – дискомфортом від зіткнення з суперечливими ідеями [46].

– Моделі ймовірності обробки інформації (Elaboration Likelihood Model - ELM): Ця модель пояснює, що переконання відбувається двома шляхами. *Центральний шлях* – це аналітична обробка аргументів (через префронтальну кору), що вимагає високої мотивації та здатності аудиторії до аналізу. *Периферійний шлях* – це обробка поверхневих сигналів (емоції, авторитет джерела, соціальний доказ, дизайн), що активує мигдалеподібне тіло (amygdala) [46]. Ефективний СтратКом повинен вміти використовувати обидва шляхи залежно від цільової аудиторії.

– Принципах впливу (Роберт Чалдіні): Шість універсальних принципів (взаємність, зобов'язання/послідовність, соціальний доказ, авторитет, приязнь, дефіцит) є тактичним інструментарієм СтратКом. Їхня кінцева мета – не маніпуляція, а побудова *довіри* [21], яка є фундаментальною валютою впливу.

На макрорівні (теорія комунікації) СтратКом спирається на [25]:

– Модель Лессвелла (1948): Класична лінійна формула «Хто (Communicator) говорить Що (Message) яким Каналом (Medium) Кому (Receiver) з яким Ефектом (Effect)». Це залишається основою для базового

планування будь-якої комунікаційної кампанії.

– Теорію двоступеневого потоку інформації (Two-Step Flow Theory): Ця теорія вказує, що мас-медіа не завжди впливають на аудиторію напряму. Вони впливають на «лідерів думок» (opinion leaders), які потім інтерпретують та ретранслюють повідомлення своїм послідовникам. Це підкреслює критичну важливість роботи з інфлюенсерами та експертною спільнотою.

– Теорію встановлення порядку денного (Agenda-Setting Theory): Медіа не обов'язково кажуть людям *що* думати, але вони надзвичайно ефективні в тому, щоб сказати їм, *про що* думати. Контроль над порядком денним є однією з ключових стратегічних цілей СтратКом.

Класичні теорії, як-от модель Лессвелла, розглядали комунікацію як лінійний, односпрямований процес: відправник «вкладає» значення у приймача. Однак сучасне інформаційне середовище (Інтернет, соціальні медіа) зруйнувало цю модель. Сучасна теорія [50] описує комунікацію як *омні-дирекційний* (всеспрямований) та *діахронічний* (безперервний у часі) процес. Комунікація – це не дискретна «подія», а «постійний потік».

У цьому новому середовищі СтратКом перетворюється на «гнучкий процес управління» («agile management process»). Його фокус зміщується з простої презентації повідомлень на «живлення цих арен» (feeding these arenas) та «тестування стратегічних рішень» у «постійному циклі зворотного зв’язку». Іншими словами, сучасний СтратКом не стільки *презентує* готову стратегію (стара модель), скільки *будує* та *перебудовує* її *через* комунікацію у реальному часі [50].

Практичний розвиток СтратКом як інструменту державної політики у сфері безпеки пройшов тривалий шлях. Модель, що домінувала в епоху Холодної війни, характеризувалася чіткою інституційною сегрегацією та «брандмауером» («firewall») між різними комунікаційними функціями [35].

– Публічна дипломатія (Public Diplomacy - PD): Це була «біла» (відкрита, атрибутована) комунікація, спрямована на іноземну аудиторію з метою просування «сприятливого погляду» на США та їхню політику [47].

Головним актором було Інформаційне агентство США (USIA), що існувало з 1953 по 1999 рік [49]. Місія USIA полягала в тому, щоб «розуміти, інформувати та впливати на іноземні суспільства», просувати американські цінності та протидіяти радянській пропаганді. Ключовими інструментами були радіостанція «Голос Америки» (VOA), програми академічних та культурних обмінів (наприклад, Fulbright), а також мережа бібліотек, видання журналів та організація виставок по всьому світу. Фокус PD був на довгостроковому будівництві відносин та «м'якої сили» [26].

– Психологічні операції (ПУОП, PSYOP): Це були «чорні» (таємні, з приховуванням джерела) або «сірі» (неатрибутовані) комунікації, що проводилися переважно військовими [35]. Їхня аудиторія – ворожі комбатанти або населення на контрольованій ворогом території. Мета була тактичною: «деморалізувати та обманути супротивника» [12], знизити його бойовий дух та схилити до капітуляції.

Існує поширений погляд на комунікації часів Холодної війни як на «золотий вік» успішної інтегрованої стратегії [48]. Однак, більш глибокий аналіз вказує, що це значною мірою «міфічне минуле». Документи Конгресу США навіть наприкінці 1980-х років – на порозі перемоги у Холодній війні – фіксують скарги на ті ж самі проблеми, що й сьогодні: *хронічне недофінансування* публічної дипломатії, *проблеми з вимірюванням ефективності* та *погана інтеграція* PD у процес формування зовнішньої політики [6]. Таким чином, проблеми координації та вимірювання ефективності є історично притаманними СтратКом. Різниця полягає в тому, що у повільнішому та сегментованому інформаційному середовищі Холодної війни ці проблеми були терпимими; у 21-му столітті вони стали критичними.

Каталізаторами фундаментальних змін у підходах до державних комунікацій стали атаки 11 вересня 2001 року (9/11) [26] та подальша «Глобальна війна з терором». США та їхні союзники раптово усвідомили, що в новому, складному та глобалізованому інформаційному середовищі [16] вони програють «битву ідей» екстремістським ідеологіям.

Поворотним моментом, який можна вважати «свідоцтвом про народження» сучасної доктрини СтратКом, стала доповідь Цільової групи Ради з питань оборонної науки США (Defense Science Board Task Force) у 2004 році. Доповідь містила жорсткий діагноз: стратегічні комунікації США перебувають «у кризі» [35].

Ключова рекомендація доповіді полягала в тому, що необхідно «вийти за межі застарілих концепцій, структурних моделей та інституційних ярликів». Документ прямо закликав до руйнування «брандмауера» Холодної війни та до глибокої «координації та активізації» раніше розділених функцій: публічної дипломатії (PD), зв'язків з громадськістю (Public Affairs - PA) та психологічних операцій (PSYOP) [35].

Причина цього краху «брандмауера» була технологічною та прагматичною. У Холодну війну сегрегація була можливою: «Голос Америки» [47] можна було транслювати для союзників, одночасно скидаючи деморалізуючі листівки [12] на ворога. Але в 21-му столітті, завдяки супутниковому телебаченню та Інтернету [16], *глобальне інформаційне середовище стало єдиним та прозорим*. Повідомлення PSYOP, призначене для деморалізації бойовиків в Іраку, через годину з'являлося на Al Jazeera і транслювалося на аудиторію в союзній Саудівській Аравії, повністю підриваючи місію публічної дипломатії (побудову довіри).

Єдиний спосіб діяти в такому прозорому середовищі – це синхронізувати *всі* комунікації та, що важливіше, *дії*. СтратКом і став цим механізмом синхронізації. Уряд США формалізував його як «координовані дії, повідомлення, образи та інші форми сигналізації... призначені для інформування, впливу або переконання обраних аудиторій на підтримку національних цілей» [48]. СтратКом перестав бути просто комунікацією; він став «лінзою, фільтром та фокусом», через який уряд повинен розглядати *всі* свої дії, від військових операцій до гуманітарної допомоги, щоб забезпечити їхню наративну узгодженість та бажаний ефект [12].

Російська агресія проти України у 2014 році стала тим шоком, що змусив

НАТО та ЄС фундаментально переглянути свої безпекові доктрини та вивести СтратКом у ранг пріоритетних інструментів відповіді.

Таблиця 1.1 – Матриця інституційних відповідей на гібридні загрози

Характеристика	*НАТО*	*Європейський Союз*	*Україна*
Ключовий доктр. документ	Стратегічна концепція 2022 [31]	Спільна рамкова програма (2016), Стратегія Безпекового Союзу (2020) [22]	Стратегія інформаційної безпеки; Рішення РНБО [69]
Визначення загрози	Гібридні тактики (дезінформація, примус) з боку конкурентів (рф, КНР) [31]	Експлуатація вразливостей нижче порогу війни [22]	Дезінформація, інформаційний тероризм, маніпуляція суспільною думкою [62]
Головна інституція СтратКом	Центр передового досвіду СтратКом (Рига) [14; 41]	East StratCom Task Force [66]; EEAS StratCom Division [43]	Центр стратегічних комунікацій та інформ. безпеки [7; 44]
Головна інституція протидії	Hybrid CoE (Гельсінкі) [14; 68]; Hybrid Analysis Branch [8]	EUvsDisinfo [66]; Гібридний синтез в рамках JRC [17]	Центр протидії дезінформації (ЦПД) при РНБО [62]
Ключові принципи відповіді	«Готуватися, стримувати, захищати»; Колективна оборона (Art. 5); Фактична комунікація [8]	«Стійкість» (Resilience); «Весь уряд» (Whole-of-government) [22]	«Весь народ» («Від волонтера до науковця»); «Доведення правди» [61]; Моральна чіткість [53]

Стратегія НАТО щодо протидії гібридним загрозам чітко артикульована як «Готуватися, Стримувати, Захищати» (Prepare, Deter, Defend). Альянс визнає, що гібридні загрози можуть досягти такого масштабу, що вимагатиме застосування Статті 5 про колективну оборону [8]. «Мозковими центрами» Альянсу у цій сфері стали Центр передового досвіду СтратКом у Ризі (Латвія) [41] та Європейський центр передового досвіду з протидії гібридним загрозам у Гельсінкі (Фінляндія) [68], де НАТО та ЄС тісно співпрацюють [14].

Ключовий доктринальний документ ризького центру, «Інструментарій стратегічних комунікацій для гібридних загроз» (Strategic Communications Hybrid Threats Toolkit), пропонує фундаментальний зсув у мисленні. СтратКом розглядається не як *реактивна* функція (відповідь на кризу), а як *проактивна*,

що вимагає «планування на основі сталого стану» («steady state baseline planning»). Мета – створити «золоту нитку стратегічного наративу» («golden thread of a strategic narrative») [18], яка б узгоджувала всі дії та комунікації уряду *до* початку кризи. НАТО наголошує на принципі протидії дезінформації «не пропагандою на пропаганду, а фактами» [8].

Підхід ЄС, що відображає його природу як регуляторної та економічної сили, зосереджений на концепції *стійкості* (resilience). Логіка проста: оскільки гібридні загрози експлуатують *вразливості* відкритого суспільства, найкращою відповіддю є посилення «імунітету» цього суспільства. Це закріплено у Спільній рамковій програмі (Joint Framework) 2016 року та Стратегії Безпекового Союзу 2020 року [22].

Інструменти ЄС включають Спільну дослідницьку комісію (JRC), що моделює гібридні загрози [17], та Оперативну робочу групу зі стратегічних комунікацій (East StratCom Task Force) [66], відому своїм проектом EUvsDisinfo. Дослідження, замовлене Європарламентом, визначає СтратКом як «ключовий фактор» протидії. Примітно, що ЄС дає широке, поведінкове визначення СтратКом: це «систематична серія стійких та узгоджених дій», спрямованих на «просування та підтримку певних типів поведінки» [43].

На перший погляд, підходи НАТО та ЄС можуть здаватися такими, що дублюються. Проте їхній аналіз виявляє чіткий та логічний розподіл праці. НАТО, як військово-політичний альянс, фокусується на *стримуванні* та *захисті* – це «щит» [8]. Їхній СтратКом спрямований на комунікацію рішучості та атрибуцію загроз військового рівня. ЄС, як регуляторна потуга, фокусується на *стійкості* – це «імунна система» [22]. Їхній СтратКом спрямований *всередину* – на зміцнення суспільства, медіаграмотність та регулювання платформ [43]. Їхня тісна співпраця є інституційним втіленням цього необхідного синтезу.

Україна з 2014 року [60] стала одночасно і головним *полігоном* для тестування російських гібридних методів, і передовою *лабораторією* зі створення та впровадження інструментів протидії. Цей досвід є унікальним, оскільки він формувався не в мирний час, а в умовах прямої агресії.

Інституціоналізація української відповіді розвивалася за двома ключовими напрямками:

– Центр протидії дезінформації (ЦПД): Створений як робочий орган Ради національної безпеки і оборони (РНБО). Це переважно операційна структура. Її функції включають: виявлення «інформаційних загроз» (понад 21 тисячу за перші чотири роки), «боротьбу з інформаційним тероризмом», а також тісну співпрацю з міжнародними партнерами (НАТО) та технологічними гігантами (Meta, Google, Tik Tok) для блокування дезінформації. ЦПД працює у зв'язці з усіма українськими спецслужбами, включаючи ГУР та СБУ [62].

– Центр стратегічних комунікацій та інформаційної безпеки (StratCom Ukraine): Цей бренд об'єднує як державну інституцію при МКІП [7], так і потужні неурядові організації. Їхня місія ширша: *реформування* та *розбудова спроможностей* державних комунікацій, навчання фахівців, розробка моделей СтратКом та реалізація стратегічних комунікаційних кампаній [44].

Знаковою подією, що кодифікувала унікальний український досвід, стала презентація у 2024 році монографії «Стратегічні комунікації в умовах війни: погляд від волонтера до науковця» [61]. Ця праця, підготовлена Національною академією СБУ спільно з представниками ГУР МОУ, волонтерами та науковцями, узагальнила досвід протидії гібридній агресії рф у 2022-2024 роках [53].

Аналіз цієї події та інституційної структури дозволяє виокремити риси «української моделі». Якщо підходи НАТО та ЄС базуються на концепції «всього уряду» («whole-of-government») [22], то українська модель, що народилася в умовах повномасштабної війни, є моделлю «всього народу» («whole-of-nation»). Сам підзаголовок монографії – «від волонтера до науковця» [61] – є ключем до розуміння. Це унікальна синергія: мережева, гнучка та високо мотивована екосистема. У ній держава (ЦПД, ГУР, СБУ) [62] встановлює стратегічні рамки та бореться із загрозами високого рівня, тоді як децентралізоване, пасіонарне громадянське суспільство (волонтери, медіа, ІТ-

спільнота) [53] веде комунікаційну війну на тактичному рівні, миттєво реагуючи на фейки та просуваючи власні наративи.

Другою фундаментальною рисою української моделі є її *ціннісна основа*. Західні теорії СтратКом часто є ціннісно-нейтральними, фокусуючись на *процесі* та *ефективності* переконання. Гібридна війна агресора, навпаки, використовує постмодерністський, релятивістський підхід: «правди не існує», «все неоднозначно» – що і є когнітивною атакою, спрямованою на створення «туману війни» [59].

Український СтратКом прямо протистоїть цьому. Як було заявлено під час презентації монографії, «Основним інструментом інформаційного протиборства є *доведення правди*» [61]. Ректор НА СБУ підкреслив, що ця боротьба – це «вибір між *світлом і темрявою*,... демократичним суспільством і диктатурою». Ця *моральна чіткість* не є слабкістю; вона є найпотужнішою зброєю. Вона (а) консолідує власне населення та (б) надає чіткий, зрозумілий наратив для міжнародних партнерів [53], що є руйнівним для стратегічної двозначності [28], яку намагається створити агресор.

Теоретико-історичний аналіз демонструє паралельну та взаємопов'язану еволюцію двох ключових концепцій безпеки 21-го століття. Гібридні загрози виникли як стратегія, що використовує синергію інструментів [23] та стратегічну двозначність [28] для атаки на когнітивний простір та процеси прийняття рішень у відкритих суспільствах [31].

Стратегічні комунікації еволюціонували у пряму відповідь на цей виклик. Вони пройшли шлях від набору сегрегованих інструментів часів Холодної війни (PD та PSYOP) [35] до інтегрованої та синхронізованої функції державної політики [12]. Ця трансформація була викликана технологічним (єдине інфо-середовище) [16] та доктринальним (звіт DSB 2004 року) усвідомленням того, що в сучасному світі кожна дія держави є комунікацією.

Таким чином, СтратКом перетворився на новий, життєво важливий інструмент стримування у «сірій зоні». Досвід НАТО, ЄС та України (Частина III) демонструє, що ефективна протидія гібридним загрозам вимагає переходу

від *реактивності* (наприклад, простого розвінчання фейків) до *проактивності*. Це означає «безперервну роботу» («steady-state») [18] зі зміцнення суспільної стійкості [22] та формування власного, потужного «стратегічного наративу», оскільки гібридна війна не має чіткого початку чи кінця.

Майбутнє СтратКом лежить у синтезі інструментів:

– Історичний урок (USIA) – довгострокове будівництво довіри через культурні та освітні програми [47].

– Доктринальний урок (США пост-9/11) – тотальна синхронізація слів та дій уряду [12].

– Інституційний урок (НАТО/ЄС) – поєднання зовнішнього «щита» (стримування) [8] та внутрішньої «імунної системи» (стійкість) [22].

– Операційний урок (Україна) – гнучка, мережева «всенародна» екосистема [53] та використання *моральної чіткості* як головної зброї проти *стратегічної двозначності* [61].

Гібридна війна – це, по суті, битва за *сприйняття* реальності. Стратегічні комунікації є мистецтвом і наукою ведення цієї битви. Теоретико-історичний аналіз беззаперечно доводить, що держава, яка у 21-му столітті не здатна синхронізувати свої дії та слова або яка втрачає довіру [21] власного населення та союзників, вже програла цю війну, незалежно від її військової чи економічної могутності.

Це, по суті, змінює саме визначення національної могутності. Традиційні показники, такі як ВВП, військовий бюджет чи кількість танків, безумовно, залишаються важливими. Проте в умовах гібридної війни вони перестають бути вирішальними, якщо держава не має «могутності наративу» – здатності формувати довіру та переконання.

Якщо гібридна війна – це атака на «соціальний клей», що тримає суспільство разом, то стратегічні комунікації стають головним інструментом його захисту та зміцнення. Це вже не допоміжна функція, а один з ключових елементів національної оборони.

Таким чином, перемога у «сірій зоні» – це не стільки військовий тріумф,

скільки досягнення стану, в якому суспільство є настільки стійким, поінформованим та об'єднаним навколо спільних цінностей, що воно просто «відштовхує» ворожі маніпуляції. Це стан, коли довіра до власних інститутів є сильнішою за будь-яку дезінформацію. І досягнення цього стану вимагає не просто реакції на загрози, а постійної, проактивної роботи зі зміцнення власної демократичної ідентичності.

РОЗДІЛ 2
МІЖНАРОДНИЙ ДОСВІД ТА ПРАКТИКА ЗАСТОСУВАННЯ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ

2.1 Правові та інституційні механізми стратегічних комунікацій у провідних країнах світу та міжнародних організаціях (НАТО, ЄС)

У сучасному геополітичному протистоянні інформаційне середовище перетворилося на повноцінний театр воєнних дій. Гібридні загрози, зокрема інформаційно-психологічні впливи, стали ключовим інструментом зовнішньої агресії. У цьому контексті стратегічні комунікації (СтратКом) еволюціонували від допоміжної функції до критично важливого елементу національної безпеки та оборони.

Ефективність стратегічних комунікацій безпосередньо залежить від чіткості інституційного дизайну, глибини доктринального обґрунтування та наявності правових механізмів для їх реалізації. Аналіз моделей НАТО, ЄС та провідних національних держав дозволяє ідентифікувати різні, але однаково цінні підходи до вирішення цього завдання.

Система стратегічних комунікацій НАТО пройшла значну еволюцію, перетворившись із набору інструментів зв'язків з громадськістю на комплексну бойову функцію. Ще на саміті у Страсбурзі/Келі було проголошено, що «дедалі важливіше, щоб Альянс комунікував у належний, своєчасний, точний та чутливий спосіб про свої мінливі ролі, цілі та місії».

Відповідно до доктрини Альянсу, СтратКом НАТО визначається як «скоординоване та належне використання комунікаційних заходів та спроможностей НАТО... на підтримку політики, операцій та діяльності Альянсу». Ця система є інтегрованою та включає п'ять ключових спроможностей [3]:

– Публічна дипломатія (Public Diplomacy): Цивільні комунікації та інформаційно-просвітницькі зусилля, спрямовані на розбудову розуміння та підтримки політики НАТО.

– Зв'язки з громадськістю (Public Affairs, PA): Цивільна взаємодія з медіа для інформування громадськості про політику та операції Альянсу.

– Військові зв'язки з громадськістю (Military Public Affairs): Інформування про військові цілі та аспекти діяльності Альянсу.

– Інформаційні операції (Information Operations, Info Ops): Спеціалізована штабна функція для координації інформаційних заходів.

– Психологічні операції (Psychological Operations, PSYOP): Сплановані заходи для впливу на сприйняття та поведінку аудиторій [5].

Наріжним каменем (keystone) доктрини Альянсу є Об'єднана союзна доктрина зі стратегічних комунікацій (Allied Joint Doctrine for Strategic Communications, AJP-10) [5]. Оновлена у 2023 році, ця доктрина представляє не просто технічний посібник, а глибокий філософський вибір.

Доктрина свідомо та міцно «прив'язує» всю комунікаційну діяльність до фундаментальних цінностей Альянсу. AJP-10 стверджує, що «вся діяльність ґрунтується на цінностях НАТО» і посилається на преамбулу Північноатлантичного (Вашингтонського) договору 1949 року: «захист свободи, спільної спадщини та цивілізації... заснованих на принципах демократії, індивідуальної свободи та верховенства права» [11].

Водночас, доктрина чітко визнає, що супротивники Альянсу (такі як росія) діють *поза* тими «правовими, етичними та моральними нормами», які є обов'язковими для членів НАТО [5]. Це створює фундаментальну асиметрію інформаційної війни. Стратегічний вибір НАТО полягає у *свідомому* веденні цієї війни *асиметрично*. Альянс принципово відмовляється від дзеркальної відповіді на дезінформацію (тобто, від використання власної пропаганди). Натомість, він використовує власну *довіру*, *прозорість*, *цінності* та *прихильність до верховенства права* як основну зброю. Це перетворює СтратКом із «битви наративів» на «битву за довіру», де факти та підтверджені

дії є ключовими боєприпасами.

Ключовим елементом в інституційній архітектурі є Центр передового досвіду НАТО зі стратегічних комунікацій у Ризі, Латвія. Він має унікальний статус: це багатонаціональна, акредитована НАТО міжнародна військова організація, яка, однак, не є частиною командної структури НАТО і не підпорядковується їй [34]. Центр фінансується країнами-учасницями [55].

Місія Центру – підтримувати спроможності НАТО через «всебічний аналіз, своєчасні поради та практичну підтримку» [10]. Його діяльність зосереджена на аналізі нових загроз, зокрема використання ворогом новітніх технологій, включаючи штучний інтелект (ШІ) та цифрові інструменти.

Ключовим досягненням Центру стала публікація у 2024 році «першої фундаментальної доктрини НАТО зі стратегічних комунікацій» («strategic communications fundamentals doctrine»). Цей документ формалізував спільну концептуальну рамку для фахівців Альянсу, ставши важливим етапом у доктринальній еволюції [41].

Операційна філософія НАТО, описана як «комплексний і узгоджений підхід», виходить далеко за межі простої реакції на дезінформацію. Її ядро – це проактивне поширення позитивних наративів, що ґрунтуються на фактах [58].

Ключова теза цього підходу полягає в тому, що Альянс не повинен намагатися реагувати на «кожну неправду», оскільки це неможливо і стратегічно програшно (це означає грати за правилами ворога). Натомість, НАТО має «чітко спрямовувати свої сигнали, робити це вчасно і рішуче». Це вимагає ідеальної «синхронізації повідомлень» усередині Альянсу та «координації з місцевими голосами» (незалежними ЗМІ, лідерами думок) [58].

Ця філософія та інституційна еволюція засвідчують тектонічний зсув. Якщо саміт 2009 року [3] говорив про СтратКом у термінах класичного PR (інформування про «ролі та цілі»), то створення StratCom COE у 2014 році [10] (безпосередньо як відповідь на агресію рф проти України) та прийняття нових доктрин у 2023-2024 роках [5], які повністю інтегрують Info Ops та PSYOP, свідчать про трансформацію. Стратегічні комунікації НАТО остаточно

еволюціонували від допоміжної *Public Affairs* функції до основної, інтегрованої *бойової функції* (warfighting function), що активно формує інформаційне середовище для досягнення політичних та військових цілей Альянсу.

Це, по суті, остаточно закріплює визнання інформаційного простору як повноцінного операційного домену, такого ж, як суша, повітря, море та кіберпростір.

Це вже не питання того, як прес-служба «розповість» про військову операцію *після* того, як вона відбулася. Це означає, що інформаційний та когнітивний ефект *вбудований* у саме планування цієї операції з першої хвилини. Військовий командир тепер зобов'язаний думати не лише про фізичний результат своїх дій, але й про те, як ці дії будуть сприйняті, який сигнал вони надішлють, і як противник намагатиметься їх викривити.

На практиці це означає, що, наприклад, розгортання батальйону НАТО на східному фланзі – це не лише військовий крок стримування. Це, перш за все, потужний, проактивний комунікаційний акт. Це спланована демонстрація рішучості, єдності та готовності до оборони. І цей сигнал має бути доставлений миттєво, чітко та синхронно усіма членами Альянсу, не залишаючи противнику часового «вікна» для того, щоб перехопити ініціативу та назвати це «ескалацією» чи «агресією».

Таким чином, НАТО свідомо прагне перехопити ініціативу в інформаційній війні. Замість того, щоб постійно реагувати, спростовувати та грати за правилами ворога, Альянс зосереджується на проактивному формуванні середовища. Він насичує інформаційний простір власним, заснованим на фактах та цінностях, наративом про оборону та безпеку. Мета полягає в тому, щоб коли (а не *якщо*) противник запустить свою дезінформаційну атаку, вона просто «не приживеться» у підготовленому, поінформованому та стійкому суспільстві.

Підхід Європейського Союзу до стратегічних комунікацій має іншу структуру та філософію, що відображає його природу як переважно політико-економічного, а не військового союзу.

Центральним органом є Європейська служба зовнішніх справ (European External Action Service – EEAS), яка використовує СтратКом для «підтримки повідомлення ЄС у різних частинах світу». На відміну від функціонального поділу НАТО (PA, PSYOP, Info Ops), інституційний дизайн ЄС є переважно географічним. Він реалізується через Робочі групи зі стратегічних комунікацій (EEAS Strategic Communication Task Forces) [13].

– East Stratcom Task Force (ESTF): Це ключова група для України. Вона фокусується на країнах Східного партнерства та Центральної Азії. ESTF не лише реагує на дезінформацію, але й веде проактивні кампанії (наприклад, «Share your Light») та підтримує стійкість суспільства до FIMI. Робота, пов'язана з Україною, є «ядром її діяльності».

– Western Balkans Task Force (WBTF): Підтримує політику ЄС у регіоні, бореться з FIMI, підтримує незалежні ЗМІ та медіаграмотність.

– Task Force South (TFS): Аналізує інфо-середовище в регіоні Близького Сходу та Північної Африки (MENA), відстежує дезінформацію та веде комунікаційні платформи, як-от «EU in Arabic».

Ця регіоналізована структура свідчить про те, що модель СтратКом ЄС структурована не навколо військових операцій (як у НАТО), а навколо *геополітичних сусідів*.

Центральним поняттям для ЄС є FIMI (Foreign Information Manipulation and Interference – Маніпулювання зовнішньою інформацією та втручання) [13]. Сама ця термінологія має оборонний характер, фокусуючись на загрозі зовнішнього втручання у демократичні процеси.

Флагманським проєктом ESTF є платформа EUvsDisinfo [54]. Вона відіграє життєво важливу роль в аналізі, документуванні та публічному викритті випадків дезінформації, зокрема російської. Діяльність EEAS значною мірою зосереджена на «підвищенні стійкості» (increasing resilience) та «підході всього суспільства» (whole of society approach), підтримуючи незалежні ЗМІ та медіаграмотність [13].

Ця модель є втіленням «м'якої сили» і є надзвичайно ефективною у

розбудові суспільної стійкості. Однак, вона несе в собі ризик потрапляння у так звану «пастку стійкості». Інституційний дизайн ЄС, зосереджений на фактчекінгу [54] та стійкості [13], практично не має «зубів» – жорстких інструментів «накладення витрат» (cost imposition), які б *карали* джерела FIMI, а не лише *парирували* їхні атаки. Цей висновок підтверджується подальшим аналізом експертних центрів.

Експертні спільноти, аналізуючи цю модель, вказують, що хоча побудова стійкості є фундаментом, вона не може бути єдиною відповіддю. Покладання виключно на стійкість, по суті, переносить увесь тягар протидії на суспільство-жертву. Це вимагає від кожного громадянина постійно бути медіаграмотним, критично мислити та перебувати у стані «інформаційної оборони».

Водночас, сам агресор, який здійснює це маніпулювання, не несе майже жодних витрат за свої дії. Він може з низькими затратами генерувати величезні обсяги дезінформації, знаючи, що найгірше, що йому загрожує – це чергове викриття на фактчекінговій платформі.

Це створює фундаментальну асиметрію. Захист (побудова стійкості) є надзвичайно дорогим, повільним та ресурсномістким процесом. Напад (створення FIMI) – дешевий, швидкий та легко масштабований.

Саме це і є «пастка стійкості». Євросоюз, зосереджуючись на зміцненні власної «імунної системи», ризикує опинитися у нескінченній грі, де він лише реагує, ніколи не змушуючи агресора заплатити ціну за саму атаку. Відсутність інструментів «накладення витрат» означає, що у джерела дезінформації немає жодних стимулів припиняти свою діяльність.

Незважаючи на різні підходи, ЄС та НАТО мають глибоке «стратегічне партнерство», засноване на «спільних цінностях». Вони «взаємно посилюють» одне одного, і їхня тісна координація є «незамінною» для євроатлантичної безпеки [15].

Аналіз національних моделей виявляє не єдиний «західний підхід», а чотири різні, хоча й сумісні, філософії інституційного дизайну СтратКом.

Фундаментальним принципом СтратКом США є співвідношення «80%

реальних дій і лише 20% слів» [64].

Офіційне визначення описує СтратКом як «сфокусовані зусилля уряду США», спрямовані на «розуміння та залучення ключових аудиторій» для «створення, зміцнення або збереження сприятливих умов» для просування інтересів держави.

Ключовим елементом є синхронізація: комунікації мають бути «синхронізовані з діями всіх інструментів національної могутності». Це інструментальний підхід, де СтратКом є важелем державної влади, що включає зв'язки з громадськістю (PA), інформаційні операції (Info Ops) та підтримку публічної дипломатії. При цьому існує висока правова та культурна чутливість до будь-яких інформаційних операцій, спрямованих на власних громадян; основний акцент робиться на заходи поза межами держави.

Саме цей принцип «80% дій» є ключовим для розуміння американської моделі. Він означає, що комунікації не створюють реальність, а лише відображають її та надають їй сенсу. На відміну від дезінформаційних моделей, які намагаються створити «віртуальну перемогу» виключно словами, американський підхід ґрунтується на тому, що найнадійніша комунікація – це реальна, видима, переконлива дія.

Наприклад, переміщення авіаносної групи, надання економічної допомоги чи укладення дипломатичного союзу – це і є ті самі «80%». Завдання стратегічних комунікацій (решта «20%») полягає в тому, щоб жодна з цих дій не була неправильно витлумачена. Вони мають забезпечити, щоб і союзники, і противники, і нейтральні спостерігачі чітко зрозуміли, *чому* ця дія відбулася і *який* сигнал вона несе.

Якщо ж слова розходяться з діями – наприклад, якщо уряд декларує одне, а його відомства роблять інше – виникає «розрив довіри». Для американської моделі, яка робить ставку на довгострокову довіру, такий розрив є стратегічною поразкою. Тому синхронізація є не просто бажаною, а абсолютно необхідною. Вона гарантує, що вся потуга держави – дипломатична, військова та економічна – рухається в одному напрямку, а комунікації виступають як «голос», що

пояснює цей рух.

Підхід Німеччини ґрунтується на нормативному, ціннісному виборі. Його ядро – це «створення власних позитивних стратегій комунікації» [57].

Німеччина свідомо та принципово «не буде долучатися до таких інструментів, як пропаганда» і відмовляється «протидіяти дезінформації за допомоги іншої дезінформації».

Ключовими інструментами є:

– Поширення «прозорої, правдивої інформації, що базується на фактах».

– Підвищення рівня медіаграмотності та критичного мислення у суспільстві.

– Підтримка незалежних ЗМІ та проєктів з громадянським суспільством.

У питаннях жорсткої протидії ФРН значною мірою покладається на загальні інструменти та мережі, доступні в рамках НАТО.

Французька модель є прикладом жорсткої бюрократичної централізації. Ключовою інституцією є Служба інформації Уряду (Service d'information du Gouvernement – SIG) [39]. Вона перебуває під прямим підпорядкуванням Прем'єр-міністра.

Основні функції SIG: 1) Аналіз громадської думки та медіа; 2) Інформування громадськості; 3) Керівництво та координація урядових комунікацій на міжвідомчому рівні.

Ця модель забезпечує максимальну узгодженість «єдиного голосу» уряду. Вона доповнюється спеціалізованими структурами, такими як агенція з онлайн-розслідувань VIGINUM та кризова міжвідомча група COLMI (Оперативний комітет з протидії інформаційним маніпуляціям) [38].

Британський підхід – це менеджерська модель, зосереджена на процесах та ефективності.

Ключовою інституцією є Урядова служба комунікацій (Government Communication Service – GCS) [42]. Вона керується Сучасною операційною

моделлю комунікацій 3.0 (Modern Communications Operating Model – MCOM) [27].

MCOM 3.0 – це цілісна система, що базується на трьох стовпах: 1) Люди та структура, 2) Політики, 3) Керівництво та інструменти.

Унікальною силою британської моделі є акцент на «Evaluation and Insight» (Оцінка та Розуміння) [42]. GCS широко використовує аналіз даних (data science) для «продемонстрування впливу» комунікацій та «спрямування мислення». Головна мета – поставити «розуміння аудиторії в основу розробки політики». Це модель, орієнтована на вимірюваний результат.

Ці чотири філософії не є взаємовиключними. Вони пропонують набір інструментів для побудови комплексної системи. Найбільш ефективна національна система СтратКом, яку могла б адаптувати Україна, була б гібридом цих моделей, що поєднує:

– Філософію «дії важливіше за слова» [64].
– Наративну стратегію «позитиву та правди» [57].
– Інституційну структуру «централізованої координації» [39].
– Механізм контролю «оцінки та аналізу даних» [42].

Наступна таблиця 2.1 синтезує ключові характеристики проаналізованих інституційних моделей.

Таблиця 2.1 – Порівняльний аналіз інституційних моделей стратегічних комунікацій

Організація / Країна	*Ключова доктрина / Підхід*	*Ключові інституції*	*Основні функції*	*Філософія протидії FIMI*
НАТО	AJP-10 (2023); «Комплексний і узгоджений підхід». Ціннісна асиметрія.	Штаб-квартира НАТО (Відділ публічної дипломатії); NATO StratCom COE (Рига); SHAPE (Військове командування).	Інтеграція PA, MilPA, PSYOP, Info Ops. Розробка доктрин. Проактивні комунікації на підтримку операцій.	Проактивна оборона та Наступ: Побудова власних наративів на основі фактів [58]; використання Info/PSYOP [3]; аналіз ворожих ТТП [41].

Продовження таблиці 2.1

Організація / Країна	*Ключова доктрина / Підхід*	*Ключові інституції*	*Основні функції*	*Філософія протидії FIMI*
Європейський Союз (ЄС)	«Підхід усього суспільства»; фокус на FIMI.	EEAS (Служба зовнішніх справ); Робочі групи (East, Balkans, South); EUvsDisinfo.	Аналіз інфо-середовища [13]; викриття дезінформації [54]; підтримка медіаграмотності; проактивні кампанії в країнах-сусідах.	Активна оборона та Стійкість: Захист демократичних процесів через підвищення суспільної стійкості (resilience) та викриття FIMI [13].
США	«80% дій, 20% слів». Синхронізація всіх інструментів нац. могутності.	Державний департамент (Global Engagement Center); Міністерство оборони (Pentagon).	Підтримка публічної дипломатії; інформаційні операції (Info Ops) [64]; зв'язки з громадськістю (PA).	Інструменталізм та Наступ: СтратКом як інструмент просування нац. Інтересів [64]. Акцент на заходах *поза межами* держави.
ФРН	«Позитивні комунікації». Відмова від пропаганди.	МЗС Німеччини; Федеральний уряд; Підрозділи протидії дезінформації.	Поширення прозорої, правдивої інформації; підвищення медіаграмотності [57]; підтримка незалежних ЗМІ та громадянського суспільства.	Нормативна оборона (Стійкість): Протидія дезінформації *правдою* та *освітою*, а не контр-пропагандою [57].
Франція	Централізована координація.	SIG (Служба інформації Уряду) (підпорядкована Прем'єр-міністру); VIGINUM; COLMI.	Міжвідомча координація комунікацій [39]; аналіз громадської думки; онлайн-розслідування (VIGINUM) [38].	Централізована оборона: Узгоджена державна відповідь на інформаційні кризи; виявлення та викриття маніпуляцій. [39; 38]
Велика Британія	MCOM 3.0. «Evaluation and Insight» (Оцінка та Розуміння).	GCS (Урядова служба комунікацій).	Розробка стандартів та політик; аналіз даних (data science) для оцінки *впливу*; розуміння аудиторії як	Менеджерська оборона (на основі даних): Використання аналізу даних для розуміння вразливостей

			основа політики [42].	аудиторії та вимірювання ефективності контр-заходів [42].

Таке поєднання дозволяє створити систему, яка є водночас гнучкою, потужною та, що найголовніше, стійкою до інформаційних атак.

Взяття за основу американського принципу «дії понад слова» та німецької «стратегії правди» означало б, що довіра стає головним активом держави. Комунікації в такій моделі не намагаються створити фальшиву реальність, а лише чітко, прозоро та переконливо пояснюють реальні дії уряду. Це автоматично позбавляє ворожу дезінформацію «кисню», адже правда, підкріплена реальними справами, є найпотужнішим захистом.

Водночас, французька модель «централізованої координації» вирішує ключову проблему «розсинхронізації», коли різні міністерства чи відомства суперечать одне одному. Вона гарантує, що вся державна машина – від військових до дипломатів – говорить «одним голосом» і рухається в одному напрямку.

І нарешті, британський підхід «оцінки та аналізу даних» слугує життєво важливим механізмом зворотного зв'язку. Він не дозволяє цій централізованій системі стати «глухою» до суспільства. Постійно аналізуючи настрої та реакції аудиторії, уряд може коригувати не лише свої *повідомлення*, але й самі *дії*, щоб вони краще відповідали потребам громадян.

У підсумку, це створює замкнений цикл: держава робить реальні, позитивні кроки, централізовано й правдиво їх пояснює, вимірює реакцію суспільства і на основі цих даних коригує свої наступні дії. Це і є модель проактивної державної політики, заснованої на довірі.

2.2 Успішні практики та міжнародний досвід у протидії гібридним інформаційно-психологічним впливам

Операція «Doppelgänger» (також відома як «RRN» – Reliable Recent News) є яскравим прикладом складної, ресурсомісткої та *триваючої* російської операції FIMI [56]. Вона керується російськими технологічними компаніями, зокрема «Агентством соціального проєктування» (Social Design Agency - SDA) та «Structura National Technologies» [37].

Її ключова тактика полягає у так званому «дзеркаленні» або «клонуванні». Оператори створюють високоякісні, візуально ідентичні копії веб-сайтів відомих та авторитетних західних медіа, таких як BILD, The Guardian, Le Monde, а також урядових порталів.

На цих фальшивих сайтах-клонах публікуються сфабриковані статті, які ідеально імітують стиль та формат справжнього видання. Цей сфабрикований контент, як правило, має на меті підірвати міжнародну підтримку України, посіяти паніку та зневіру серед європейського населення або посилити внутрішньополітичний розкол у країнах-союзниках.

Завершальний етап – це поширення. Ці фейкові статті масово «розганяються» через широку, часто автоматизовану, мережу акаунтів у соціальних мережах, зокрема у X (колишньому Twitter) та Facebook. Мета полягає в тому, щоб обманом змусити користувача повірити, ніби він читає новину з надійного джерела, і таким чином «відмити» дезінформацію, вводячи її у публічний дискурс.

Кампанія демонструє еволюцію російських методів, поєднуючи технології та психологічні маніпуляції:

– Клонування та Імітація (Impersonation): Операція створює високоякісні *клони* (двійники) веб-сайтів авторитетних західних ЗМІ (наприклад, Bild, 20minutes, The Guardian, а також українського RBC Ukraine) та урядових порталів (наприклад, МЗС Франції або навіть НАТО) [56].

– Генерація контенту: Для наповнення цих сайтів фейковими статтями, прес-релізами та коментарями широко використовується *генеративний штучний інтелект*.

– Поширення та Ампіліфікація: Контент поширюється через розгалужені *мережі ботів* та *скоординовану неавтентичну поведінку* в соціальних мережах, насамперед на платформі X (колишній Twitter), де було виявлено до 88% активності цієї мережі [1].

Цілі операції – маніпулювання громадською думкою в Європі, підрив довіри до урядів, дискредитація підтримки України та прямий вплив на демократичні процеси, зокрема на вибори до Європейського парламенту 2024 року [56].

Сама ця тактика «клонування» є психологічно надзвичайно ефективною. Вона не намагається створити новий, невідомий бренд, якому потрібно було б місяцями завойовувати довіру. Натомість, вона паразитує на довірі, яку авторитетні медіа та уряди будували десятиліттями.

Операція робить ставку на те, що у швидкісному світі соціальних мереж пересічний користувач реагує на знайомий логотип та візуальний стиль, не перевіряючи ретельно адресу сайту. Таким чином, він несвідомо сприймає фейковий, маніпулятивний контент як перевірений, легітимний матеріал від джерела, якому він звик довіряти.

Використання штучного інтелекту для генерації контенту при цьому вирішує для агресора ключову проблему – проблему масштабу. Якщо раніше для створення переконливої брехні кількома мовами були потрібні значні людські ресурси, то зараз ШІ дозволяє продукувати величезні обсяги правдоподібних, граматично коректних текстів майже миттєво та з мінімальними витратами.

Це перетворює дезінформацію з поодиноких «вкидів» на безперервний, промисловий потік, спрямований на ерозію реальності. Мета такої операції – не стільки переконати аудиторію в якійсь одній конкретній неправді, скільки створити стан загального інформаційного хаосу, втоми та цинізму. Коли

громадяни остаточно втрачають здатність відрізняти правду від вигадки і перестають довіряти будь-яким джерелам, вони стають ідеально вразливими до маніпуляцій, а суспільна здатність до ухвалення раціональних рішень – паралізованою.

Урок 1: Атака на довіру, а не на факти. Тактика «Doppelgänger» є значно витонченішою, ніж просто поширення брехні. Вона імітує джерела, яким аудиторія вже довіряє [37]. Психологічна мета полягає не в тому, щоб змусити читача повірити в одну конкретну фейкову новину. Мета – змусити його сумніватися у кожному джерелі. Коли The Guardian (справжній) спростовує фейк з The Guardian (клонованого), у свідомості пересічного громадянина обидва джерела починають асоціюватися з дезінформацією.

Таким чином, «Doppelgänger» демонструє, що сучасна FIMI – це не просто створення фейкових новин, а спроба створення фейкової реальності. Вона атакує не факти, а довіру – фундаментальну операційну систему демократичного суспільства. Клонуючи надійні бренди, росія намагається зруйнувати саме поняття надійного джерела, перетворюючи інформаційне середовище на хаотичне та неговірне поле.

Це і є кінцева мета – досягнення стану «когнітивного паралічу» суспільства. Коли інформаційне поле перетворюється на «дзеркальну кімнату», де неможливо відрізнити оригінал від підробки, громадяни втрачають головний інструмент демократії – спільну, узгоджену реальність.

Якщо неможливо домовитися про базові факти, то стає неможливим і будь-який конструктивний політичний діалог чи прийняття спільних рішень. У цей вакуум довіри проникають найрадикальніші наративи, теорії змови та емоційні маніпуляції.

Суспільство, яке більше нікому не вірить, стає не стійким, а цинічним та апатичним. Воно втрачає здатність до колективної дії, до мобілізації та до опору. І саме в цьому стані паралічу та внутрішнього розбрату агресор може найлегше досягти своїх реальних політичних та військових цілей, адже жертва, по суті, виявляється знерухомленою зсередини.

Урок 2: Викриття не дорівнює стримуванню. Кампанія була детально викрита консорціумом організацій, зокрема EU DisinfoLab, ще у 2022 році [37]. Про неї звітували уряди (зокрема Франції [38]) та структури ЄС. Однак у 2024 році Європейська служба зовнішніх справ (EEAS) випускає звіт під промовистою назвою «“Доппельгангер” завдає удару у відповідь» [56], деталізуючи його атаки на європейські вибори.

Це доводить ключовий засвоєний урок: викриття не є стримуванням. Пасивна, оборонна діяльність (фактчекінг, публікація звітів), яку проводить EUvsDisinfo, є життєво важливою для інформування, але вона не зупиняє саму операцію. Агресор (в даному випадку «Social Design Agency» [37]) просто враховує викриття і адаптує тактику. Цей висновок прямо підводить до наступного, найважливішого уроку, сформульованого експертними центрами.

Цей найважливіший урок полягає у необхідності накладення витрат. Сам факт того, що операція «Doppelgänger» продовжується навіть після повного викриття, доводить, що для її організаторів ціна такої діяльності залишається прийнятною. Викриття у медіа чи урядові звіти сприймаються ними не як поразка, а лише як «операційні витрати» або тимчасова незручність, яку легко компенсувати зміною тактики.

Таким чином, оборонна стратегія «стійкості», хоч і є важливою, виявляється фундаментально недостатньою. Вона, по суті, перекладає весь тягар протидії на суспільство-жертву, вимагаючи від нього постійної пильності.

Справжнє стримування починається лише тоді, коли агресор розуміє, що за кожну таку атаку він заплатить реальну, болючу ціну. Це вимагає від держав-жертв переходу від пасивного інформування до проактивних дій: запровадження жорстких санкцій проти конкретних компаній та осіб, причетних до FIMI, юридичного переслідування, дипломатичного тиску та навіть дзеркальних технічних заходів. Лише тоді, коли вартість операції перевищить її потенційну користь, агресор буде змушений зупинитися, а не просто «завдати удару у відповідь».

Hybrid CoE (Гельсінкі), що тісно співпрацює з ЄС та НАТО [40], є

ключовим аналітичним центром, який надає глибокий аналіз гібридних загроз [33]. Його останні звіти містять фундаментальні висновки для розробки політики СтратКом.

Звіт Hybrid CoE Research Report 15 (жовтень 2025 р.) «Протидія дезінформації в євроатлантичному регіоні: сильні сторони та прогалини» базується на анкетуванні країн-членів ЄС та НАТО [24].

Він виявляє три критичні «прогалини» (Gaps):

– Дефіцит ресурсів: Практики на місцях вважають, що їхня робота *недостатньо забезпечена ресурсами*.

– Розрив з громадянським суспільством: Існує *брак налагоджених механізмів співпраці* між урядовими органами та недержавним сектором (фактчекерами, НУО).

– Стратегічний перекіс у бік «стійкості»: Це ключовий висновок. Країни роблять набагато більше для *підвищення обізнаності* (resilience), але *значно менше* для *«обмеження або покарання винуватців»*.

Цей останній висновок є фундаментальним. Він означає, що поточна євроатлантична стратегія є незбалансованою та, по суті, пасивною. Вона зосереджена на тому, щоб зробити жертву сильнішою, але майже нічого не робить для того, щоб зробити агресора слабшим.

Такий підхід, де-факто, легітимізує дезінформацію як безризиковий інструмент зовнішньої політики. Агресор бачить, що його операції, навіть у разі викриття, не призводять до жодних болючих наслідків. Максимум, що йому загрожує, – це черговий звіт чи спростування.

Це створює ситуацію, в якій держави-члени ЄС і НАТО змушені витрачати величезні, постійно зростаючі ресурси на нескінченну «гонку озброєнь» у сфері медіаграмотності та фактчекінгу. Водночас агресор, витрачаючи значно менше, продовжує свої атаки, знаючи, що за це не буде жодного реального покарання. Таким чином, звіт чітко підводить до висновку, що без механізмів «накладення витрат» – санкцій, юридичного переслідування та інших проактивних заходів – сама по собі стратегія «стійкості» приречена на

стратегічний програш.

Hybrid CoE Paper 25 (серпень 2025 р.) «Перетворення стратегії на практику: Уроки стримування гібридних загроз» базується на аналізі настільних ігор (wargames) зі стримування [36].

Цей звіт формулює головний урок для західних демократій: небезпека «надмірної залежності від стійкості» (over-reliance on resilience).

Аналіз доводить, що надмірна залежність від стійкості та «уникнення ескалації» (що є природним для демократій, які дотримуються норм) насправді «запрошує до експлуатації» (invites exploitation) з боку ворожих акторів. Якщо агресор знає, що єдиною відповіддю на його атаку буде черговий звіт про медіаграмотність або спростування фейку, він не має жодних стимулів припиняти атаку.

Ці два звіти [24] ідеально доповнюють один одного. Звіт 15 діагностує проблему (ми не караємо). Звіт 25 пояснює наслідки (оскільки ми не караємо, нас експлуатують).

Це перетворює гібридну агресію на надзвичайно привабливу, «дешеву» стратегію з низьким ризиком та високою потенційною винагородою. Агресор може «мацати» оборону, проводити операції, втручатися у процеси, знаючи, що найгірше, що йому загрожує, – це публічне викриття, яке він може просто ігнорувати.

Таким чином, звіт чітко підводить до висновку, що стримування не може базуватися лише на обороні. Справжнє стримування вимагає довіри до того, що на ворожу дію надійде адекватна відповідь, яка накладе на агресора витрати – політичні, економічні чи репутаційні.

Якщо демократії лише зміцнюють свою «стійкість», вони, по суті, погоджуються постійно «терпіти удар». Вони показують, що готові нескінченно посилювати свій захист, але ніколи не дадуть відповідь, яка змусить нападника заплатити ціну. І саме ця передбачувана відсутність покарання робить гібридні атаки неминучими та постійними.

Рекомендація Hybrid CoE є однозначною: необхідна збалансована

стратегія, що поєднує «розбудову стійкості» (resilience-building) з «надійним накладенням витрат» (credible cost imposition) [36].

Це найважливіший урок міжнародного досвіду після 2014 року. «Накладення витрат» у контексті СтратКом – це не лише загальні економічні санкції [40]. Це означає перехід від *пасивної* німецької моделі [57] та *оборонної* моделі ЄС [13] до *активної* інструментальної моделі США [64] та НАТО [3], яка інституційно включає *наступальні* спроможності – інформаційні [4] та психологічні [5] операції.

Стратегічний імператив для будь-якої держави, що протистоїть гібридним загрозам – це *перебалансування* свого портфеля СтратКом. Вона повинна підтримувати компонент «стійкості» (Оборона), одночасно *розбудовуючи* інституціоналізований компонент «накладення витрат» (Наступ).

Іншими словами, держава, що зосереджена виключно на стійкості, по суті, погоджується вести війну лише на власній території. Вона постійно перебуває в обороні, гасячи інформаційні «пожежі», які створює агресор. Це стратегічно програшна позиція, оскільки ініціатива завжди залишається у нападника.

Компонент «накладення витрат» докорінно змінює цю динаміку. Його мета – перенести бойові дії в інформаційний та когнітивний простір самого супротивника.

Замість того, щоб нескінченно спростовувати фейки про себе, держава починає проактивно висвітлювати правду про агресора: його злочини, його корупцію, його внутрішні суперечності та брехливість його власної системи. Це змушує агресора самого переходити до оборони, витрачати величезні ресурси на спростування та виправдання вже на *своїй* території.

Таким чином, «накладення витрат» – це не про помсту, а про відновлення стратегічного балансу. Це єдиний спосіб змусити агресора заплатити реальну ціну за свої дії, вирватися з пастки реактивності та, зрештою, зробити гібридну агресію невигідною для нього.

У пошуках міжнародного досвіду важливо усвідомити, що Україна сама

була і залишається ключовим джерелом цього досвіду для Заходу.

Аналіз публікацій НАТО засвідчує, що Альянс почав вивчати досвід України негайно після початку агресії 2014 року. Ключовою публікацією стала книга «Countering Hybrid Threats: Lessons Learned from Ukraine» («Протидія гібридним загрозам: Уроки, засвоєні з України») [9].

Ця книга стала результатом семінару НАТО Advanced Research Workshop (ARW), що відбувся у Бухаресті ще у вересні 2015 року. Семінар зібрав 50 експертів, включаючи політиків, практиків зі спецслужб та науковців, для вивчення природи конфлікту в Україні. Книга містить 28 статей, що детально аналізують тактику гібридної війни в Україні, російські інформаційні та психологічні операції, кіберзагрози та наслідки для євроатлантичної безпеки [9].

Відбувається *циркуляція досвіду*. «Міжнародний досвід», який Україна зараз прагне адаптувати, значною мірою *був сформований* на основі аналізу «українського досвіду» 2014-2021 років. Саме гібридна війна росії проти України стала каталізатором створення NATO StratCom COE у Ризі в 2014 році [10] та подальшої еволюції доктрини НАТО AJP-10 [11]. Це означає, що Україна є не просто *реципієнтом* міжнародної допомоги, а й *ключовим генератором* знань у сфері протидії гібридним загрозам.

Однак повномасштабне вторгнення 2022 року кардинально змінило цю динаміку, перетворивши Україну з об'єкта *вивчення* гібридних атак на живу *лабораторію* всеохопної державної та суспільної стійкості.

Якщо до 2022 року Захід аналізував переважно українські поразки та вразливості у «сірій зоні», то новий етап продемонстрував безпрецедентну модель успішного опору. Міжнародна спільнота тепер вивчає не стільки *проблему*, скільки українські *рішення*, які генеруються в режимі реального часу.

Досвід України після 2022 року – це вже не просто тактика протидії дезінформації. Це модель тотальної мобілізації суспільства, де державні інституції, громадянське суспільство, волонтери та приватний сектор об'єдналися у єдину мережеву екосистему опору. Саме тому, вивчаючи

міжнародний досвід, ми маємо чітко усвідомлювати: Україна не лише наздоганяє партнерів, але й у багатьох аспектах формує та випереджає світові тренди у сфері інформаційної та когнітивної війни.

Цей новий досвід, здобутий в умовах тотальної конвенційної війни, продемонстрував світові унікальну модель, де стратегічні комунікації перестали бути виключною прерогативою держави. Вони стали «всенародною справою».

Ми побачили безпрецедентний синергетичний ефект, де офіційні заяви Президента чи Міністерства оборони миттєво підхоплювалися, доповнювалися та поширювалися горизонтальною мережею волонтерів, незалежних медіа, IT-фахівців та мільйонів звичайних громадян.

Більше того, Україна відмовилася грати у «сірій зоні» стратегічної двозначності, яку нав'язував ворог. Вона протиставила російській брехні та маніпуляціям максимально чіткий, заснований на правді та моральних імперативах наратив – наратив боротьби за свободу, демократію та власне існування.

Саме ця гнучкість, мережевість та моральна чіткість стали тим новим «українським уроком», який зараз активно вивчається і адаптується західними структурами, що прагнуть знайти ефективну відповідь на глобальні гібридні виклики.

РОЗДІЛ 3
ПРІОРИТЕТНІ НАПРЯМИ ВДОСКОНАЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ УКРАЇНИ У СФЕРІ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ ДЛЯ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ

3.1 Прогалини та можливості адаптації міжнародного досвіду до української системи публічного управління

Україна, перебуваючи в стані повномасштабної війни з 2022 року (і гібридної з 2014-го) [70], створила розгалужену систему протидії інформаційним загрозам.

Ключовими суб'єктами є Центр протидії дезінформації (ЦПД), що діє при Раді національної безпеки і оборони (РНБО), та Центр стратегічних комунікацій та інформаційної безпеки (ЦСКІБ, «Spravdi») [55]. ЦПД активно позиціонується як ключовий партнер для NATO StratCom COE. ЦСКІБ («Spravdi») був створений при Міністерстві культури та інформаційної політики, але наприкінці 2025 року було оголошено про його передачу під управління Кабінету Міністрів України [2].

Ця інституційна архітектура, з двома потужними, але окремими центрами, свідчить про глибоке усвідомлення загрози на різних рівнях.

З одного боку, існування Центру протидії дезінформації при РНБО підкреслює, що держава розглядає інформаційні атаки як пряму загрозу національній безпеці, що вимагає залучення всього силового та безпекового блоку.

З іншого боку, перепідпорядкування «Spravdi» безпосередньо Кабінету Міністрів є надзвичайно важливим кроком. Це виводить стратегічні комунікації зі статусу галузевої політики (під Міністерством культури) на рівень загальнодержавної урядової координації. Теоретично, це дає Центру

повноваження для синхронізації дій усіх міністерств та органів виконавчої влади.

Однак така двоелементна система неминуче створює фундаментальний виклик – проблему чіткої координації та розподілу повноважень між самим ЦПД (який є частиною вертикалі РНБО) та «Spravdi» (який тепер діє по горизонталі уряду). Без чіткого механізму синхронізації існує ризик дублювання функцій, конкуренції за ресурси або, що найнебезпечніше, надсилання неузгоджених, розсинхронізованих сигналів як всередині країни, так і назовні.

Незважаючи на значні досягнення цих структур, порівняльний аналіз з найкращими міжнародними практиками виявляє п'ять фундаментальних прогалин:

Прогалина 1: Інституційна фрагментація та нестабільність. Постійна зміна підпорядкування ЦСКІБ (від одного міністерства до іншого, а тепер – до КабМіну) [2] свідчить про відсутність усталеної, стабільної інституційної моделі та, ймовірно, про конкуренцію за вплив. Це ускладнює реалізацію «політики одного голосу» та призводить до тематичної фрагментації комунікацій [70]. Відсутній єдиний, наділений реальними повноваженнями міжвідомчий координаційний центр.

Ця відсутність єдиного, наділеного реальними повноваженнями, центру призводить до прямої «розсинхронізації» на операційному рівні. В умовах швидкої інформаційної кризи, різні державні органи – військові, дипломатичні та безпекові – можуть почати комунікувати паралельно. Вони ризикують поширювати сигнали, які не узгоджені між собою, а іноді навіть суперечать один одному.

Це створює «інформаційний шум» вже всередині країни, який дезорієнтує як власне населення, так і міжнародних партнерів, які не розуміють, яка саме позиція є офіційною.

Замість потужного, консолідованого державного наративу, який би формував порядок денний, виникає дисонанс. Такий стан не лише підриває

довіру до влади, але й змушує витрачати дорогоцінний час та ресурс на внутрішнє «узгодження позицій» вже *після* того, як ворожа атака відбулася. Це повністю позбавляє державу можливості діяти проактивно.

Прогалина 2: Стратегічний перекіс у бік «оборони» (реактивності). Аналіз публічної діяльності ЦПД [55] та ЦСКІБ [2] засвідчує абсолютне домінування захисних функцій: «спростування фейків», «аналіз російських наративів», «викриття ворожих ІПСО», «навчання OSINT» [51]. Це підтверджує висновок, зроблений ще у 2019 році: СтратКом в Україні часто помилково сприймається як PR-кампанія або антипропаганда, а не як «стратегічне планування» та «побудова власного національного наративу» [65].

Така модель, зосереджена на обороні, неминуче прирікає державу на втрату стратегічної ініціативи. Замість того, щоб проактивно формувати власний порядок денний, українські комунікаційні інституції змушені постійно «наздоганяти» ворога, реагуючи на ті теми, які він свідомо «вкидає» в інформаційний простір.

Навіть успішне спростування фейку – це все одно дія, що відбувається в рамках, нав'язаних агресором. Увага суспільства та міжнародних партнерів прикута до *теми, яку обрав ворог*, а не до тієї, яку хотіла б просувати Україна.

Це створює небезпечний «наративний вакуум». Поки основні ресурси йдуть на боротьбу з брехнею, бракує зусиль на те, щоб будувати та просувати власну позитивну історію – історію про цілі України, її цінності та її бачення майбутнього. В результаті, у свідомості аудиторії «боротьба з росією» починає переважати над чітким розумінням того, за *що саме* бореться Україна. Це робить суспільство більш вразливим до втоми та зневіри, оскільки оборона без чітко артикульованої мети виснажує.

Прогалина 3: Потрапляння у «пастку стійкості» (відповідність діагнозу Hybrid CoE). Поточна українська модель є ідеальною ілюстрацією «прогалини», ідентифікованої Hybrid CoE у звіті [24]. Існує сильний, добре розвинений фокус на стійкості та обізнаності суспільства [2]. Однак, в публічному полі практично відсутній чіткий інституційний компонент, відповідальний за «обмеження або

покарання винуватців». Система перевантажена функціями «щита» і практично не має інституціоналізованого «меча». Це створює стратегічну асиметрію, яка робить Україну вразливою до «експлуатації», про яку застерігає Hybrid CoE [36].

Ця асиметрія, по суті, дає агресору «вільні руки». Він отримує можливість безкарно, знову і знову, проводити свої операції, знаючи, що найгірше, що йому загрожує – це чергове спростування у медіа.

Це перетворює інформаційну війну на гру «в одні ворота». Агресор із низькими витратами генерує нескінченний потік дезінформації, змушуючи українську державну машину витрачати величезні ресурси, щоб просто «гасити пожежі».

У довгостроковій перспективі, така виключно оборонна позиція веде до стратегічного виснаження. Суспільство втомлюється від нескінченного потоку загроз, а держава, не маючи «меча», не може перехопити ініціативу. Вона не може змусити ворога самого перейти до оборони та почати витрачати ресурси на захист вже *свого* власного інформаційного простору.

Прогалина 4: Розрив з громадянським суспільством. Хоча співпраця ЗСУ та держорганів з громадянським суспільством існує і є життєво важливою [63], вона часто є ситуативною. Відсутні формалізовані, сталі, інституціоналізовані механізми щоденної співпраці та обміну даними між урядовими структурами та недержавним сектором (НУО, фактчекерами). Це точно відповідає другій «прогалині», ідентифікованій Hybrid CoE [24].

Такий *ситуативний*, а не інституційний, підхід означає, що держава фактично не використовує один зі своїх найпотужніших активів.

Громадянське суспільство, з його гнучкістю, швидкістю реакції та часто вищою довірою у нішевих аудиторіях, залишається «недоінтегрованим» у загальну систему національної безпеки. Замість того, щоб створити єдину, потужну екосистему, де державні центри та незалежні фактчекери щоденно й автоматично обмінюються даними та синхронізують зусилля, ми отримуємо «паралельну гру».

Урядові структури та громадські організації часто змушені дублювати роботу один одного, витрачаючи обмежені ресурси на аналіз одних і тих самих загроз. Це створює неефективність та уповільнює реакцію. У той час як неузгоджена система витрачає дорогоцінний час на координацію «вручну» вже під час кризи, агресор безперешкодно продовжує свої операції, використовуючи цю незлагодженість проти нас.

Прогалина 5: Відсутність системи M&E (Моніторингу та Оцінки). Жоден з проаналізованих українських документів [70] не згадує про впровадження системи вимірювання ефективності та впливу комунікацій. Успіх досі вимірюється кількісними показниками (кількість спростованих фейків, охоплення), а не якісними (реальна зміна громадської думки, підвищення рівня довіри до інституцій, зміна поведінки цільових аудиторій). Це унеможливлює стратегічне планування, яке є основою британської моделі GCS [42].

Без такої системи оцінки державні комунікаційні структури, по суті, діють «наосліп». Вони не мають жодних об'єктивних даних, щоб зрозуміти, чи їхні зусилля *взагалі працюють*, чи вони просто «виробляють контент».

Це призводить до неминучого марнування обмежених ресурсів. Величезні зусилля можуть витрачатися на спростування фейків, яке, наприклад, не досягає потрібної аудиторії. Або, що ще гірше, воно може випадково *посилювати* ворожий наратив, знайомлячи з ним тих, хто раніше про нього не чув.

Таким чином, унеможливлюється будь-яке стратегічне навчання та адаптація системи. Вона не може вчитися на своїх помилках або масштабувати свої успіхи, оскільки вона просто не здатна їх надійно ідентифікувати. В результаті, комунікації застрягають на рівні тактичної метушні та звітування про кількість, замість того, щоб еволюціонувати у справжній інструмент досягнення вимірюваного впливу на реальність.

Ідентифіковані прогалини можуть бути ефективно усунені шляхом цілеспрямованої адаптації міжнародних моделей, проаналізованих раніше. Оптимальна модель для України в умовах тотальної війни – це «гібрид

гібридів», що поєднує найкращі елементи різних підходів.

На інституційному рівні, це означає відхід від поточної фрагментації на користь жорсткої централізованої координації, подібної до французької моделі SIG. Україні потрібен не просто ще один аналітичний центр, а єдиний, наділений реальними повноваженнями, міжвідомчий орган. Цей орган, що перебував би під прямим керівництвом найвищої виконавчої влади, мав би мандат на синхронізацію комунікацій *усіх* державних акторів – від Збройних Сил до дипломатів – забезпечуючи «політику одного голосу».

На операційному рівні, ця система має подолати «пастку стійкості», перейшовши від суто реактивної німецької моделі до проактивної американської філософії. Комунікації мають не лише спростовувати брехню, але й просувати власний порядок денний, спираючись на принцип «80% дій – 20% слів». Це означає інституціоналізацію «меча» – компоненту «накладення витрат», який би проактивно працював у інформаційному просторі противника, замість нескінченної оборони на власній території.

Водночас, щоб ця централізована та проактивна машина не стала «глухою» і не почала працювати «в холосту», вона повинна бути збалансована британською моделлю M&E. Необхідно впровадити жорстку систему моніторингу та оцінки ефективності, яка б вимірювала не кількість прес-релізів, а реальний вплив на довіру та поведінку цільових аудиторій.

І, нарешті, вся ця «гібридна» структура має стояти на непохитному фундаменті німецького ціннісного підходу – абсолютній прихильності до правди. Саме поєднання централізованої координації, проактивних дій та оцінки ефективності, заснованих на правді, дозволить трансформувати український СтратКом з реактивного «щита» на повноцінний інструмент досягнення стратегічної переваги.

Для прогалини 1 (Фрагментація) - Адаптація французької моделі SIG [39]. Оголошена передача ЦСКІБ під Кабінет Міністрів [2] є унікальною можливістю. Цей орган не повинен стати «ще одним міністерством». Він має бути перетворений на аналог французького SIG – компактний, але надзвичайно

впливовий міжвідомчий координаційний центр при голові виконавчої влади. Його завдання – не дублювати аналітику ЦПД чи роботу прес-служб, а стратегічно спрямовувати та синхронізувати комунікації всіх органів влади.

Це означає, що коли виникає чутлива криза або з'являється важлива стратегічна можливість, саме цей новий орган має забезпечувати, щоб Міністерство оборони, Міністерство закордонних справ та розвідувальні служби говорили одним, узгодженим голосом.

Він не повинен писати за них прес-релізи, але він має встановлювати загальні ключові повідомлення, темп та «червоні лінії» для всіх. Така жорстка централізована координація є єдиним способом покласти край ситуаціям, коли різні гілки влади, навіть з найкращими намірами, ненавмисно суперечать одна одній.

Саме цей «інформаційний хаос», створений власною розсинхронізацією, ворог негайно використовує для просування наративів про «некомпетентність» та «розкол» української влади. Отже, такий орган має діяти як «диригент» урядового оркестру, маючи прямий мандат від найвищого керівництва, щоб гарантувати, що всі грають за одними нотами.

Для прогалин 2 і 3 (Перекіс у «захист» / «Пастка стійкості») - Адаптація моделей Hybrid CoE [36] та США [64]. Це вимагає трьох кроків:

– Проактивний наратив: Впровадити німецьку філософію «позитивних комунікацій» [57] для розробки та просування *власного* довгострокового національного наративу (наративу перемоги, відбудови, справедливості) [63], замість постійного реагування на порядок денний ворога.

– Синхронізація: Жорстко поєднати цей наратив з американським принципом «80% дій, 20% слів». Кожне комунікаційне повідомлення (напр., про боротьбу з корупцією або відбудову) має бути негайно підкріплене *реальною, відчутною дією* уряду чи ЗСУ.

– Накладення витрат: Виконати рекомендацію Hybrid CoE та розпочати інституціоналізацію *наступальних* інформаційних спроможностей за доктринами НАТО (зокрема, AJP-10.1 (Info Ops) [4]) для активного

«накладення витрат» на джерела FIMI, а не лише на їхні продукти.

Це означає фундаментальну зміну філософії – перехід від «гри в обороні» до «гри на випередження».

Поки держава лише спростовує фейки (що є реакцією), вона завжди буде на крок позаду. Ворог диктує порядок денний, змушуючи нас витрачати ресурси на теми, які обрав він.

Впровадження проактивного наративу, підкріпленого реальними діями, дозволяє Україні самій стати «ньюсмейкером». Замість того, щоб пояснювати, чому ми *не* корумповані, держава має показувати реальні посадки, а комунікації мають це чітко пояснювати. Це і є «синхронізація дії та слова».

Однак, навіть цього недостатньо, якщо агресор продовжує свої атаки безкарно. Саме тут вступає в дію третій елемент – накладення витрат. Це означає, що паралельно з розбудовою власної «позитивної історії», держава має активно і болісно бити по джерелах ворожої дезінформації.

Замість того, щоб просто заблокувати сайт «RRN» (Doppelgänger), цей підхід вимагає проведення операцій, які б викривали та паралізували роботу самого «Агентства соціального проєктування» в росії. Це змушує ворога переходити до оборони вже у *своєму* інформаційному просторі, витрачати ресурси на захист, а не на напад.

Таким чином, поєднання цих трьох кроків – позитивний наратив, підкріплений діями, та проактивне «полювання» на джерела загроз – є єдиним способом вирватися з «пастки стійкості» та перетворити СтратКом на справжній інструмент перемоги.

Для прогалини 4 (Розрив з НУО) Адаптація рекомендацій ОБСЄ 40 та усунення «прогалини» Hybrid CoE [24].

Необхідно створити формальні, сталі платформи для взаємодії між державними інституціями (ЦПД, ЦСКІБ, ЗСУ) та громадянським суспільством [63]. Це напряму вирішує «прогалину», ідентифіковану Hybrid CoE, та перетворює ситуативну співпрацю на надійний «загальносуспільний» механізм.

Створення таких формальних платформ перетворює співпрацю з епізодичної та особистісної (що тримається на контактах окремих людей) на інституційну та систематичну.

Коли співпраця є ситуативною, вона є крихкою. Вона залежить від особистих стосунків і може розпастися під час кадрових змін або у момент гострої кризи, коли немає часу на «ручну» координацію.

Натомість, формалізована платформа – це постійно діючий, «всепогодний» механізм. Він забезпечує двосторонній обмін інформацією в режимі реального часу. Громадські організації, які часто є гнучкішими та мають глибшу експертизу у вузьких сферах, отримують канал, щоб миттєво передавати свої знахідки «нагору» – до державних аналітичних центрів.

У свою чергу, державні органи отримують можливість не просто реагувати на ці звіти, а й використовувати ці довірені мережі для поширення та «заземлення» своїх стратегічних наративів. Це дозволяє поєднати легітимність та ресурси держави з довірою та гнучкістю громадянського суспільства, створюючи єдину, значно потужнішу екосистему протидії, де сильні сторони кожного учасника посилюють загальний результат.

Для прогалини 5 (Відсутність M&E) Адаптація британської моделі GCS [42].

Необхідно створити в рамках оновленого, централізованого ЦСКІБ окремий підрозділ «Evaluation and Insight» («Оцінка та Розуміння») за британською моделлю MCOM 3.0 [42]. Його завдання – за допомогою аналізу даних (включаючи соціологію та data science) перейти від кількісних показників (охоплення) до якісних (зміна рівня довіри, зміна поведінки аудиторії). Це дозволить ухвалювати рішення на основі даних, а не інтуїції.

Такий підхід, заснований на даних, докорінно змінює саму природу роботи. Замість того, щоб просто «гасити пожежі» та звітувати про кількість виробленого контенту, система отримує можливість стратегічно навчатися.

Вона зможе чітко бачити, які саме наративи *не* працюють, які повідомлення викликають зворотний ефект, а які – навпаки, знаходять

найбільший відгук у конкретних цільових групах. Це дозволить відмовитися від неефективних, але ресурсномістких кампаній, і сфокусувати обмежені державні ресурси виключно на тих діях, що доведено призводять до реальних, вимірюваних змін у сприйнятті та довірі.

Таким чином, «оцінка та розуміння» стає не просто функцією звітності. Вона перетворюється на стратегічний компас усієї державної комунікаційної машини, що дозволяє їй адаптуватися, еволюціонувати та, зрештою, вигравати битву за довіру, спираючись на докази, а не на припущення.

3.2 Посилення інституційної спроможності та ефективності національної системи стратегічних комунікацій

На основі проведеного аналізу прогалин та можливостей, пропонуються п'ять пріоритетних практичних рекомендацій для реформування державної політики у сфері стратегічних комунікацій.

Рекомендація 1: Інституційна реформа та централізація координації (Адаптація: Франція)

Дія: Завершити передачу Центру стратегічних комунікацій (ЦСКІБ) [2] під пряме підпорядкування Кабінету Міністрів України (або, альтернативно, Апарату РНБО, але з чітким відокремленням від функцій ЦПД).

Мандат: Наділити цей оновлений Центр статусом *головного міжвідомчого координаційного органу* (за аналогією з французьким SIG [39]) з чіткими повноваженнями для *стратегічного спрямування* та *синхронізації* комунікацій всіх міністерств, відомств та військово-цивільних адміністрацій [63]. Він має стати «нервовим центром» уряду, що забезпечує «політику одного голосу».

Структура: Створити в рамках оновленого ЦСКІБ департамент «Аналізу та Оцінки» (Insight and Evaluation) за британською моделлю GCS [42]. Цей

департамент має впровадити єдину державну методологію M&E (Моніторингу та Оцінки) для аналізу *ефективності* та *впливу* комунікацій на цільові аудиторії, надаючи зворотний зв'язок для коригування державної політики.

Ключова перевага цієї моделі полягає саме у поєднанні централізованого керування (французька модель) із вбудованим механізмом зворотного зв'язку (британська модель).

Сама по собі централізація вирішує лише проблему «одного голосу». Вона припиняє хаос, коли різні відомства суперечать одне одному, що є критично важливим для усунення інституційної фрагментації. Однак, без потужної системи «Оцінки та Розуміння», цей центральний орган ризикує перетворитися на «чорну скриньку» – структуру, що транслює єдиний, але абсолютно неефективний сигнал, відірваний від реальних настроїв суспільства.

Саме додавання британського компоненту M&E перетворює цю структуру з простого «координатора» на «мозок» системи. Цей орган отримує «очі та вуха» – здатність бачити, як його рішення впливають на довіру людей. Це дозволяє миттєво коригувати стратегію, відмовляючись від того, що не працює, та посилюючи те, що дає реальний, вимірюваний результат у зміні поведінки чи підвищенні довіри.

Рекомендація 2: Створення «Подвійного Ядра»: Балансування «Стійкості» та «Накладення витрат» (Адаптація: Hybrid CoE)

Дія: Інституційно та функціонально розмежувати захисні («Щит») та проактивні/наступальні («Меч») функції СтратКом, усуваючи асиметрію. Закріпити за ЦПД [55] та відповідним крилом ЦСКІБ [2] функції оборонного контр-FIMI. Їхні завдання: моніторинг загроз, викриття (за моделлю EUvsDisinfo [54]), публічне спростування, розробка національних програм медіаграмотності (адаптуючи німецький досвід [57]) та «щеплення» суспільства від дезінформації [63]. Створити (або інституціоналізувати існуючі спроможності в структурах ГУР МО, СБУ, ССО) окремий Міжвідомчий центр проактивних інформаційних операцій.

Мета: Виконання рекомендації Hybrid CoE [36] щодо «надійного

накладення витрат».

Функції: Планування та виконання операцій (відповідно до доктрин НАТО, як AJP-10.1 (Info Ops) [4]) проти джерел FIMI (таких як «Social Design Agency» [37] та їхня інфраструктура), а також просування українських наративів на ворожих та нейтральних територіях [63].

Таке чітке функціональне розмежування є абсолютно вирішальним. Воно, по суті, звільняє оборонні, публічні структури («Щит») від завдань, які суперечать самій їхній природі.

Головна зброя «Щита» – це довіра. А довіра будується виключно на прозорості та стовідсотковій прихильності до правди, як це демонструє німецька модель. Розділення функцій дозволяє цим оборонним центрам (ЦПД та «Spravdi») повністю зосередитися на зміцненні довіри та стійкості всередині суспільства, не компрометуючи себе «сірими» чи непублічними операціями.

Водночас, окремий проактивний центр («Меч») отримує «розв'язані руки» для виконання зовсім іншої, специфічної роботи. Йому більше не потрібно оглядатися на публічність чи займатися просвітництвом. Його єдине завдання – діяти: планувати та виконувати операції, які змусять ворога самого переходити до оборони. Його ціль – не спростовувати фейкові сайти «Doppelgänger», а зробити так, щоб саме «Агентство соціального проєктування», яке їх створює, припинило своє існування або його діяльність стала надто дорогою та ризикованою.

Саме така «двоядерна» структура нарешті створює той самий баланс, якого вимагає Hybrid CoE. «Щит» гарантує, що суспільство є захищеним, а «Меч» гарантує, що агресор починає платити реальну ціну за кожну атаку. Це перетворює інформаційну війну з гри «в одні ворота», де ми лише захищаємось, на повноцінний двосторонній конфлікт, де ми нарешті можемо перехопити ініціативу.

Рекомендація 3: Перехід до проактивної наративної політики (Адаптація: США).

Дія: Сформувати в рамках оновленого координаційного ЦСКІБ постійну

Наративну групу (Narrative Group) для розробки, тестування та імплементації довгострокових стратегічних наративів України [63].

Принцип: Впровадити як обов'язковий стандарт державної комунікації американську модель «80% дій, 20% слів» [64]. Кожна позитивна комунікація (наратив «Перемога», наратив євроінтеграції, наратив відбудови) має бути синхронізована з реальними, відчутними діями Уряду та Сил Оборони. Це єдиний шлях до відновлення та зміцнення довіри.

Стратегія: Прийняти німецьку філософію «позитивних комунікацій» [57]. Державні комунікатори мають фокусуватися на просуванні власного правдивого, позитивного порядку денного, а не постійно перебувати в реакції на брехню ворога.

Це поєднання є, по суті, формулою відновлення довіри. Воно докорінно змінює саму функцію державних комунікацій – з «реагування на брехню» на «пояснення реальних дій».

Коли держава діє за принципом «80% дій, 20% слів», сам факт дії (наприклад, успішна військова операція, ухвалення важливого антикорупційного закону, відкриття відбудованої школи) стає головним комунікаційним актом. «Двадцять відсотків слів» у цьому випадку – це не пропаганда, а лише чітке, правдиве та вчасне пояснення того, що відбулося і чому це важливо.

Такий підхід, заснований на правді, автоматично «деактивує» ворожі наративи. Замість того, щоб втягуватися у нескінченні та виснажливі суперечки з ворогом (граючи за його правилами), держава просто створює нову, позитивну реальність, яку неможливо спростувати.

Коли громадяни та міжнародні партнери бачать, що слова уряду не розходяться з ділом, рівень довіри зростає. І саме ця відновлена довіра стає найміцнішим «щитом» проти будь-яких майбутніх інформаційних атак. Ворожа брехня просто не зможе «прижитися» у суспільстві, яке довіряє своїм інституціям, бо воно бачить результати їхньої реальної роботи.

Рекомендація 4: Побудова «Загальносуспільного» підходу (Адаптація:

ОБСЄ)

Дія: Створити формальну, постійно діючу платформу (наприклад, Спільний координаційний комітет) для співпраці, координації та захищеного обміну інформацією між державними органами (ЦПД, ЦСКІБ, МОУ, МЗС) та громадянським суспільством (ключовими незалежними фактчекерами, НУО, волонтерськими рухами, аналітичними центрами) [63].

Обґрунтування: Цей крок напряму вирішує «прогалину №2», ідентифіковану Hybrid CoE [24] – «брак налагоджених механізмів співпраці». Це посилить довіру та ефективність «підходу всього суспільства» [13], який є критично важливим для протидії гібридним загрозам.

Така інституціоналізація, по суті, перетворює ситуативні альянси на стабільну екосистему.

Це вирішує фундаментальну проблему неефективності та дублювання зусиль. Коли співпраця є ситуативною, вона залежить від особистих контактів і часто активується вже після того, як криза почалася. В результаті, державні органи та громадські організації можуть паралельно аналізувати одну й ту саму загрозу, марнуючи дорогоцінний час та обмежені ресурси.

Формальна платформа створює постійно діючий, захищений «конвеєр» для обміну даними. Це стає вулицею з двостороннім рухом: недержавний сектор, який часто є більш гнучким та швидким, отримує канал для негайної передачі своїх знахідок «нагору», безпосередньо до центрів прийняття рішень. У свою чергу, держава отримує можливість використовувати довірені канали громадських організацій для поширення своїх повідомлень та наративів, що часто є більш ефективним, ніж пряма державна комунікація.

Таким чином, держава отримує не просто «допомогу» від волонтерів, а повноцінного, інтегрованого партнера. Це і є практичне втілення «загальносуспільного» підходу, де легітимність та ресурси держави поєднуються з гнучкістю, швидкістю та довірою громадянського суспільства.

Рекомендація 5: Поглиблена інтеграція в євроатлантичні структури

Дія 1: Прискорити процес технічного та політичного приєднання України

до Системи швидкого сповіщення ЄС (EU Rapid Alert System – RAS), що забезпечить обмін даними про загрози FIMI в режимі реального часу. Ця необхідність була ідентифікована ще у 2019 році [65].

Дія 2: Запровадити постійну програму обміну та стажування (а не лише короткострокових візитів [55]) для фахівців ЦПД, ЦСКІБ та профільних підрозділів Сил Оборони у NATO StratCom COE (Рига) та Hybrid CoE (Гельсінкі).

Це забезпечить двосторонній обмін. Україна отримає прямий доступ до новітніх доктрин [41], тренінгів (включаючи ШІ) та методологій. Натомість Україна надасть партнерам безцінний практичний досвід повномасштабної інформаційної війни [9], посилюючи власну роль як генератора знань у сфері євроатлантичної безпеки.

Такий двосторонній обмін є, по суті, найвищою формою інституціоналізації досвіду. Він переводить співпрацю з рівня ситуативних контактів та «обміну ввічливостями» на рівень повної оперативної сумісності.

Для України це означає, що її фахівці припиняють «винаходити велосипед». Замість того, щоб вчитися виключно на власних, часто болісних, помилках, вони отримують прямий доступ до десятиліть напрацьованих і стандартизованих процедур НАТО та ЄС. Приєднання до Системи швидкого сповіщення ЄС (RAS) – це не просто отримання доступу до ще одного «чату», це повна інтеграція у спільний кровообіг європейської безпеки.

Для партнерів з НАТО та ЄС цінність є не меншою. Їхні доктрини та настільні ігри (wargames), про які згадувалося раніше, – це переважно *теорія* або досвід протидії «сірій зоні». Україна ж пропонує їм безпрецедентний, унікальний досвід *тотальної* війни – живої «лабораторії», де їхні теоретичні моделі проходять перевірку реальним боєм.

Таким чином, цей обмін перестає бути стосунками «вчителя та учня». Він перетворюється на спільну еволюцію. Західні партнери отримують життєво важливі дані для адаптації своїх доктрин до умов війни 21-го століття, а Україна, натомість, не просто отримує допомогу, а на практиці доводить свою

роль як незамінного та повноцінного учасника євроатлантичної системи безпеки.

Таблиця 3.1 – Матриця адаптації міжнародного досвіду для посилення СтратКом України

Ідентифікована прогалина в Україні	*Рекомендована дія*	*Міжнародна модель / «Засвоєний урок»*	*Ключові джерела*
Інституційна фрагментація, нестабільність підпорядкування [70; 2].	Рекомендація 1: Створення єдиного координаційного центру (ЦСКІБ) при КМУ з реальними повноваженнями.	Французька модель SIG (централізована міжвідомча координація при голові виконавчої влади).	[39; 63; 2]
Відсутність системи вимірювання ефективності (M&E), фокус на «кількості», а не «впливі».	Рекомендація 1 (частина 2): Створення департаменту «Оцінки та Розуміння» (Insight & Evaluation) в ЦСКІБ.	Британська модель GCS / MCOM 3.0 (вимірювання впливу на аудиторію через data science).	[42]
Стратегічний перекіс у «захист» [51]; Потрапляння у «пастку стійкості» [24].	Рекомендація 2: Створення «Подвійного Ядра» – інституціоналізація «Меча» (компоненту «накладення витрат»).	Урок Hybrid CoE (Paper 25) (надмірна стійкість «запрошує до експлуатації») [36]; Доктрина НАТО AJP-10.1 (Info Ops) [4].	[3; 4; 24; 36]
Реактивність комунікацій; відсутність власного довгострокового наративу [65].	Рекомендація 3: Створення постійної «Наративної групи»; впровадження принципу «80% дій, 20% слів».	Німецька модель («позитивні комунікації») [57] + Модель США («синхронізація з діями») [64].	[64; 57; 65]
Розрив з громадянським суспільством (брак *формалізованих* механізмів).	Рекомендація 4: Створення формальної, постійно діючої платформи для співпраці «держава-НУО».	Прогалина, ідентифікована Hybrid CoE (Report 15) [24]; Рекомендації ОБСЄ [52].	[24; 63; 52]
Недостатня інтеграція в механізми ЄС/НАТО; обмін досвідом має «реципрокний» характер.	Рекомендація 5: Приєднання до EU RAS; запровадження постійних програм обміну з StratCom COE та Hybrid CoE.	Урок «Циркуляції досвіду» (Україна як генератор знань для НАТО) [9]; Потреба в інтеграції в RAS [65].	[55; 41; 9; 65]

Сукупне впровадження цих п'яти рекомендацій означає не просто «ремонт» чи покращення поточної системи. Це є повна стратегічна трансформація усього державного підходу до інформаційної та когнітивної війни.

Це системний перехід від моделі, яка наразі є фрагментованою, реактивною та переважно оборонною, до моделі, яка є централізованою, проактивною та збалансованою.

Головний ефект такого реформування – це вихід із «пастки стійкості», в якій Україна змушена нескінченно та виснажливо «гасити пожежі», реагуючи на порядок денний, який нав'язує ворог. Натомість, пропонується перехоплення стратегічної ініціативи.

Створення «подвійного ядра» («Щита» і «Меча») дозволяє одночасно робити дві критично важливі речі, які зараз неможливі. «Щит», який спирається на правдиві, позитивні наративи та реальні дії («80% дій, 20% слів»), отримує змогу відбудовувати та зміцнювати найголовніший актив – довіру власного суспільства та міжнародних партнерів. Саме ця довіра, а не кількість спростованих фейків, є справжнім імунітетом до дезінформації.

Водночас, інституціоналізація «Меча» нарешті змушує агресора платити ціну. Це перетворює інформаційну війну з гри «в одні ворота» на повноцінний двосторонній конфлікт, де ворог змушений сам переходити до оборони, витрачати ресурси на захист вже *свого* інформаційного простору.

При цьому централізація координації за французькою моделлю та інтеграція з громадянським суспільством гарантують, що вся ця потужна машина діє синхронно, як єдиний організм. А британська модель оцінки ефективності стає тим «компасом», який не дозволяє цій системі працювати «вхолосту», постійно звіряючи її дії з реальним впливом на довіру та поведінку людей.

Таким чином, виконання цих рекомендацій перетворює СтратКом з допоміжної функції «зв'язків з громадськістю» на один з ключових інструментів досягнення перемоги – такий самий, як збройні сили чи дипломатія. Це створює систему, де Україна нарешті перестає бути лише об'єктом атак і стає повноцінним, потужним гравцем у глобальній битві за реальність.

ВИСНОВКИ

У ході виконання магістерської роботи було проведено комплексний аналіз міжнародного досвіду у сфері стратегічних комунікацій для протидії гібридним загрозам. Поставлена мета дослідження, що полягала у розробці науково обґрунтованих рекомендацій щодо вдосконалення державної політики України, є досягнутою. Усі визначені завдання було послідовно виконано, що дозволило сформулювати наступні висновки.

1. З'ясовано, що поняття «гібридна війна» еволюціонувало від початкової тактичної концепції Френка Хоффмана (синергетичне поєднання конвенційних, іррегулярних та злочинних методів) до сучасної стратегічної парадигми. Після 2014 року ключовою характеристикою гібридних загроз стала «стратегічна двозначність», спрямована не стільки на фізичне знищення, скільки на параліч когнітивної сфери та процесів прийняття рішень супротивника. Встановлено, що гібридна війна – це атака на саму систему ліберальної демократії, що ведеться у «сірій зоні» через цілеспрямовану експлуатацію її сильних сторін (відкрита преса, верховенство права) як вразливостей.

2. Проаналізовано, що стратегічні комунікації як відповідь на ці загрози базуються на теоретичних засадах соціальної психології (управління сприйняттям, моделі переконання) та теоріях комунікації (встановлення порядку денного). Історичний розвиток СтратКом пройшов шлях від сегрегованої моделі часів Холодної війни («брандмауер» між «білою» публічною дипломатією та «чорними» психологічними операціями) до інтегрованої моделі пост-9/11. Технологічна революція (єдине інфо-середовище) та доктринальні зміни (звіт Ради з питань оборонної науки США 2004 року) перетворили СтратКом на «лінзу» для синхронізації усіх дій та слів уряду. Досвід України після 2014 року сформував унікальну «всенародну» модель, що використовує моральну чіткість як головну зброю проти

стратегічної двозначності.

3. Систематизовано та охарактеризовано ключові міжнародні інституційні моделі.

– НАТО розглядає СтратКом як інтегровану бойову функцію, засновану на Об'єднаній союзній доктрині зі стратегічних комунікацій та принципі «ціннісної асиметрії» (протидія пропаганді фактами та правдою).

– ЄС фокусується на «стійкості» та географічному підході (робочі групи Європейської служби зовнішніх справ), однак ця модель несе ризик потрапляння у «пастку стійкості» (захист без накладення витрат на агресора).

– Національні моделі включають: американську (інструментальна, «80% дій, 20% слів»), німецьку (нормативна, «стратегія правди» без пропаганди), французьку (бюрократична централізація «одного голосу» через Службу інформації Уряду) та британську (менеджерська, фокус на вимірюванні впливу через моніторинг та оцінку).

4. Узагальнено ключові «засвоєні уроки» з міжнародної практики. Аналіз операції «Doppelgänger» (клонування сайтів) доводить, що її метою є атака на довіру до інститутів, а не на факти. Головний урок цієї операції полягає в тому, що «викриття не дорівнює стримуванню», оскільки агресор продовжує діяльність, адаптуючи тактику. Звіти Європейського центру передового досвіду з протидії гібридним загрозам – підтверджують цей висновок, діагностуючи в західних підходах «надмірну залежність від стійкості», яка «запрошує до експлуатації». Таким чином, міжнародний досвід доводить: ефективна стратегія неможлива без компонента «надійного накладення витрат» на агресора.

5. Виявлено п’ять фундаментальних прогалин в українській системі публічного управління у сфері СтратКом:

– Інституційна фрагментація: наявність двох центрів (Центр протидії дезінформації та Центр стратегічних комунікацій та інформаційної безпеки) без єдиного, наділеного реальними повноваженнями, координаційного органу створює ризик «розсинхронізації».

– Стратегічний перекіс у «захист»: система працює в реактивному режимі (спростування фейків), віддаючи стратегічну ініціативу ворогові.

– Потрапляння у «пастку стійкості»: поточна модель ідеально ілюструє діагноз Європейського центру передового досвіду з протидії гібридним загрозам – сильний «щит» (стійкість), але майже повна відсутність інституціоналізованого «меча» (накладення витрат).

– Розрив з громадянським суспільством: співпраця є ситуативною, а не інституціоналізованою, що веде до дублювання функцій та неефективності.

– Відсутність системи моніторингу та оцінки: успіх вимірюється кількісними показниками (охоплення, кількість фейків), а не якісними (зміна довіри чи поведінки), що унеможливлює стратегічне планування.

6. Обґрунтовано пріоритетні напрями та надано п’ять практичних рекомендацій щодо реформування системи. Рекомендовано створення «гібридної» моделі, що поєднує найкращі міжнародні практики:

– Централізувати координацію (адаптація французької моделі Служби інформації Уряду) та впровадити систему моніторингу та оцінки (адаптація британської моделі Урядової служби комунікацій).

– Створити «Подвійне Ядро» (урок Європейського центру передового досвіду з протидії гібридним загрозам), чітко розмежувавши публічний «Щит» (стійкість) та непублічний «Меч» (наступальні операції з «накладення витрат» за доктринами НАТО).

– Перейти до проактивної наративної політики, поєднавши американський принцип «80% дій, 20% слів» з німецькою «стратегією правди».

– Формалізувати співпрацю з громадянським суспільством через створення постійних інституційних платформ.

– Поглибити інтеграцію в євроатлантичні структури, приєднавшись до Системи швидкого сповіщення ЄС та запровадивши постійні програми обміну з Центром передового досвіду НАТО зі стратегічних комунікацій та Європейським центром передового досвіду з протидії гібридним загрозам.

Загалом, впровадження цих рекомендацій дозволить трансформувати

національну систему стратегічних комунікацій з фрагментованої та реактивної на централізовану, проактивну та збалансовану, перетворивши її на повноцінний інструмент досягнення стратегічної переваги та перемоги у гібридній війні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 3rd EEAS Report on Foreign Information Manipulation and Interference Threats. *European External Action Service*. 2025. March. URL: https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf (last accessed: 06.11.2025).

2. 4 роки діяльності: команда Центру з Міністерством культури та стратегічних комунікацій. Підсумки і результати. *SPRAVDI*. 2025. 05 квіт. URL: https://spravdi.gov.ua/4-roky-diyalnosti-komandy-czentru-z-ministerstvom-kultury-ta-strategichnyh-komunikaczij-pidsumky-i-rezultaty/ (дата звернення: 06.11.2025).

3. About Strategic Communications. *NATO Strategic Communications Centre of Excellence*. URL: https://stratcomcoe.org/about_us/about-strategic-communications/1 (last accessed: 06.11.2025).

4. Allied Joint Doctrine for Information Operations (AJP-10.1). *GOV.UK*. 2023. 2 Feb. URL: https://www.gov.uk/government/publications/allied-joint-doctrine-for-information-operations-ajp-101 (last accessed: 06.11.2025).

5. Allied Joint Doctrine for Strategic Communications (AJP-10). *GOV.UK*. 2023. 29 March. URL: https://www.gov.uk/government/publications/allied-joint-doctrine-for-strategic-communications-ajp-10 (last accessed: 06.11.2025).

6. Center S. The Evolution of American Public Diplomacy: Four Historical Insights. *US Advisory Commission on Public Diplomacy*. 2013. 2 Dec. URL: https://2009-2017.state.gov/pdcommission/meetings/218815.htm (last accessed: 05.11.2025).

7. Centre for Strategic Communication and Information Security. *Wikipedia*. URL: https://en.wikipedia.org/wiki/Centre_for_Strategic_Communication_and_Information_Security (last accessed: 05.11.2025).

8. Countering hybrid threats. *NATO*. 2024. 07 May. URL: https://www.nato.int/cps/en/natohq/topics_156338.htm (last accessed:

05.11.2025).

9. *Countering hybrid threats: lessons learned from Ukraine* / N. Iancu, A. Fortuna, C. Barna (eds.). Amsterdam : IOS Press, 2016. Vol. 128. URL: https://www.nato.int/cps/en/natohq/topics_142012.htm (last accessed: 06.11.2025).

10. Decoding the Information Environment: NATO's Strategic Communications Centre of Excellence. *NATO's ACT*. 2024. 18 Sept. URL: https://www.act.nato.int/article/stratcom-coe-2024/ (last accessed: 06.11.2025).

11. Defence Strategic Communications Vol. 15. 2025. URL: https://stratcomcoe.org/publications/download/DSC_VOL_15.pdf (last accessed: 06.11.2025).

12. Eder M. Strategic Communication: Key To Deterrence And Defense. *War Room*. 2025. 24 July. URL: https://warroom.armywarcollege.edu/articles/deterrence-and-defense/ (last accessed: 05.11.2025).

13. EEAS Strategic Communication Task Forces. *European Union*. URL: https://www.eeas.europa.eu/eeas/eeas-strategic-communication-task-forces_en (last accessed: 06.11.2025).

14. EU And NATO Welcome Hybrid CoE. *NATO StratCom COE*. URL: https://stratcomcoe.org/news/eu-and-nato-welcome-hybrid-coe/105 (last accessed: 05.11.2025).

15. EU-NATO strategic partnership. *European External Action Service*. URL: https://www.eeas.europa.eu/eeas/eu-nato-strategic-partnership_en (last accessed: 06.11.2025).

16. Freeman B. R. The Role of Public Diplomacy, Public Affairs, and Psychological Operations in Strategic Information Operations. Naval Postgraduate School, 2005. URL: https://apps.dtic.mil/sti/tr/pdf/ADA435691.pdf (last accessed: 05.11.2025).

17. Giannopoulos G., Smith H., Theocharidou M. The Landscape of Hybrid Threats: A conceptual model. Ispra : European Commission, 2020. 52 p. URL: https://euhybnet.eu/wp-content/uploads/2021/06/Conceptual-Framework-Hyb

rid-Threats-HCoE-JRC.pdf (last accessed: 05.11.2025).

18. Gill M., Heap B., Hansen P. Strategic Communications Hybrid Threats Toolkit / ed. B. Heap ; NATO Strategic Communications Centre of Excellence. Riga : NATO StratCom COE, 2021. 46 p. URL: https://stratcomcoe.org/publications/download/Strategic-Communications-Hybrid-Threats-Toolkit.pdf (last accessed: 05.11.2025).

19. Hoffman F. G. Conflict in the 21st century: The rise of hybrid wars. Arlington, VA : Potomac Institute for Policy Studies, 2007. 51 p. URL: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf (last accessed: 05.11.2025).

20. Hoffman F. G. Examining complex forms of conflict. *Prism*. 2018. Vol. 7, No. 4. P. 30–47. URL: https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1983462/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/ (last accessed: 05.11.2025).

21. How Strategic Communication is Key to Influence. *Clear Points Messaging LLC*. 2020. 7 July. URL: https://clearpointsmessaging.com/communication-in-the-workplace-how-strategic-communication-creates-foundation-of-influence/ (last accessed: 05.11.2025).

22. Hybrid threats / European Commission. URL: https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en (last accessed: 05.11.2025).

23. Käihkö I. The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession. *Parameters*. 2021. Vol. 51, No. 3. DOI: 10.55540/0031-1723.3084.

24. Kalenský J., Hanhijärvi H. Countering disinformation in the Euro-Atlantic: Strengths and gaps. *Hybrid CoE Research Report*. 2025. No. 15. URL: https://www.hybridcoe.fi/publications/countering-disinformation-in-the-euro-atlantic-strengths-and-gaps/ (last accessed: 06.11.2025).

25. Key Models and Theories in Strategic Communication. *YouAccel*. URL: https://youaccel.com/lesson/key-models-and-theories-in-strategic-communicat

ion/premium (last accessed: 05.11.2025).

26. Lim Y. J. Theorizing Strategic Communication in Parsimony from the US government perspective. *Kome*. 2015. Vol. 3, No. 1. URL: https://scholarworks.utrgv.edu/cgi/viewcontent.cgi?article=1032&context=com_fac (last accessed: 05.11.2025).

27. Modern Communications Operating Model 3.0. *GOV.UK*. URL: https://www.communications.gov.uk/modern-communications-operating-model-3-0/ (last accessed: 06.11.2025).

28. Mumford A. Ambiguity in hybrid warfare. *Hybrid CoE Strategic Analysis*. 2020. No. 24. URL: https://www.hybridcoe.fi/wp-content/uploads/2020/09/202009_Strategic-Analysis24-1.pdf (last accessed: 05.11.2025).

29. Mumford A., Carlucci P. Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security*. 2023. Vol. 8, No. 2. P. 192–206. DOI: https://doi.org/10.1017/eis.2022.19.

30. Nickerson C. Impression management: Erving Goffman theory. *Simply Psychology*. 2022. URL: https://www.simplypsychology.org/impression-management.html (last accessed: 05.11.2025).

31. North Atlantic Treaty Organization. NATO 2022 Strategic Concept. Brussels : NATO Headquarters, 2022. 11 p. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf (last accessed: 05.11.2025).

32. Perception management. *Wikipedia*. URL: https://en.wikipedia.org/wiki/Perception_management (last accessed: 05.11.2025).

33. Publications of the Hybrid CoE. *Hybrid CoE*. URL: https://www.hybridcoe.fi/all-publications/ (last accessed: 06.11.2025).

34. Publications of the NATO StratCom COE. *NATO Strategic Communications Centre of Excellence*. URL: https://stratcomcoe.org/publications (last accessed: 06.11.2025).

35. *Report of the Defense Science Board Task Force Strategic Communication* / Defense Science Board Task Force. September 2004. URL:

https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/05-F-0422.pdf (last accessed: 05.11.2025).

36. Rusinaitė V. Turning Strategy into Praxis: Lessons in Hybrid Threat Deterrence. *Hybrid CoE Research Report*. 2025. No. 14. URL: https://www.hybridcoe.fi/publications/turning-strategy-into-praxis-lessons-in-hybrid-threat-deterrence/ (last accessed: 06.11.2025).

37. Russian disinformation campaign 'Doppelgänger' unmasked: A web of deception. *U.S. Cyber Command*. 2024. 29 Oct. URL: https://www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgnger-unmasked-a-web-of-deception/ (last accessed: 06.11.2025).

38. Russian information manipulation networks targeting Ukraine and its partners. *Ministère de l'Europe et des Affaires étrangères*. 2024. 22 Feb. URL: https://www.diplomatie.gouv.fr/IMG/pdf/a4_dp-vs_desinfo-ukraine_eng_web-22-02-24_cle48c1c1.pdf (last accessed: 06.11.2025).

39. Service d'information du Gouvernement (SIG). *Gouvernement.fr*. URL: https://www.info.gouv.fr/organisation/service-d-information-du-gouvernement-sig (last accessed: 06.11.2025).

40. Shagina M. Lessons Learned from Western Sanctions on Russia: Knowing Your Target Well. *Hybrid CoE Strategic Analysis*. 2023. No. 35. URL: https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-35-lessons-learned-from-western-sanctions-on-russia-knowing-your-target-well/ (last accessed: 06.11.2025).

41. Shaping the Future of Strategic Communications in NATO. *NATO's ACT*. 2025. 16 Oct. URL: https://www.act.nato.int/article/stratcom-coe-2025/ (last accessed: 05.11.2025).

42. Strategic communication: a behavioural approach. *GOV.UK*. URL: https://www.communications.gov.uk/guidance/strategic-communication/ (last accessed: 06.11.2025).

43. Strategic communications as a key factor in countering hybrid threats / J. P. Villar García, C. Tarín Quirós, J. Blázquez Soria, C. Galán Pascual, C. Galán

Cordero. Brussels : European Union, 2021. (PE 656.323). DOI: 10.2861/14410. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656323/EPRS_STU(2021)656323_EN.pdf (last accessed: 05.11.2025).

44. StratCom Ukraine - центр стратегічних комунікацій. *StratCom Ukraine*. URL: https://stratcomua.org/ (дата звернення: 05.11.2025).

45. Surowiec P. Strategic communications and public diplomacy. *ASEF Public Diplomacy Handbook*. Singapore : Asia-Europe Foundation, 2021. P. 22–34. URL: https://www.researchgate.net/publication/357476836_Strategic_Communications_and_Public_Diplomacy (last accessed: 05.11.2025).

46. The Science Behind Persuasion: How Strategic Communication Shapes Public Opinion. *Hubbard School of Journalism & Mass Communication*. 2025. 25 June. URL: https://hsjmc.umn.edu/news/2025-06-25-science-behind-persuasion-how-strategic-communication-shapes-public-opinion (last accessed: 05.11.2025).

47. United States Information Agency. *Wikipedia*. URL: https://en.wikipedia.org/wiki/United_States_Information_Agency (last accessed: 05.11.2025).

48. United States Strategic Communication. *Wikipedia*. URL: https://en.wikipedia.org/wiki/United_States_Strategic_Communication (last accessed: 05.11.2025).

49. USIA Collection. *Roper Center at Cornell University*. URL: https://ropercenter.cornell.edu/usia (last accessed: 05.11.2025).

50. Van Ruler B. Communication theory: An underrated pillar on which strategic communication rests. *Future directions of strategic communication* / H. Nothhaft, K. P. Werder, D. Verčič, A. Zerfass (eds.). Routledge, 2020. P. 39–53. DOI: https://doi.org/10.1080/1553118X.2018.1452240.

51. Боротьба з російською брехнею та формування позиції держави: підсумки роботи Центру стратегічних комунікацій у 2024 році. *SPRAVDI*. 2025. 08 січ. URL: https://spravdi.gov.ua/borotba-z-rosijskoyu-brehneyu-ta-formuvannya-pozycziyi-derzhavy-pidsumky-roboty-czentru-strategichnyh-komunikaczij-u-2024-roczi/ (дата звернення: 06.11.2025).

52. Взаємодія Збройних сил України з громадянським суспільством: довідник / Кравченко Л.О., Нікітюк Т.А., Лукічов В.Л., Арнаутова В.В.; за заг. ред. Л.О. Кравченко. К., 2021. 48 с. URL: https://www.osce.org/files/f/documents/4/4/510533.pdf (дата звернення: 06.11.2025).

53. Вийшла книга про український досвід стратегічних комунікацій в умовах війни. *Детектор медіа*. 2024. 25 листоп. URL: https://detector.media/infospace/article/235146/2024-11-25-vyyshla-knyga-pro-ukrainskyy-dosvid-strategichnykh-komunikatsiy-v-umovakh-viyny/ (дата звернення: 05.11.2025).

54. Глосарій: Хто є хто в зоопарку FIMI. *EUvsDisinfo*. URL: https://euvsdisinfo.eu/ua/%D0%B3%D0%BB%D0%BE%D1%81%D0%B0%D1%80%D1%96%D0%B9-%D1%85%D1%82%D0%BE-%D1%94-%D1%85%D1%82%D0%BE-%D0%B2-%D0%B7%D0%BE%D0%BE%D0%BF%D0%B0%D1%80%D0%BA%D1%83-fimi/ (дата звернення: 06.11.2025).

55. Директор Центру передового досвіду стратегічних комунікацій НАТО Яніс Сартс відвідав Україну з офіційним візитом. *Центр протидії дезінформації*. URL: https://cpd.gov.ua/events/dyrektor-czentru-peredovogo-dosvidu-strategichnyh-komunikaczij-nato-yanis-sarts-vidvidav-ukrayinu-z-oficzijnym-vizytom/ (дата звернення: 06.11.2025).

56. Доппельгангер завдає удару у відповідь: розкриття діяльності FIMI, спрямованої на вибори до ЄП. *EUvsDisinfo*. 2024. 19 черв. URL: https://euvsdisinfo.eu/ua/%D0%B4%D0%BE%D0%BF%D0%BF%D0%B5%D0%BB%D1%8C%D0%B3%D0%B0%D0%BD%D0%B3%D0%B5%D1%80-%D0%B7%D0%B0%D0%B2%D0%B4%D0%B0%D1%94-%D1%83%D0%B4%D0%B0%D1%80%D1%83-%D1%83-%D0%B2%D1%96%D0%B4%D0%BF/ (дата звернення: 06.11.2025).

57. Із дезінформацію треба боротися позитивними комунікаційними стратегіями – посол ФРН. *Укрінформ*. 2021. 7 груд. URL: https://www.ukrinform.ua/rubric-society/3364651-iz-dezinformaciu-treba-borotisa-pozitivnimi-komunikacijnimi-strategiami-posol-frn.html (дата звернення:

06.11.2025).

58. Комплексний, узгоджений підхід до стратегічної комунікації. *NATO Review*. 2023. 16 берез. URL: https://www.nato.int/docu/review/uk/articles/2023/03/16/kompleksnij-uzgodyoenij-pdhd-do-strategchno-komunkats/index.html (дата звернення: 06.11.2025).

59. Лобода Ю. О. Поняття «гібридна війна (гібридні військові дії)»: походження та складність. *Наука і оборона*. 2020. № 4. С. 20–23. DOI: https://doi.org/10.33099/2618-1614-2020-13-4-20-23.

60. Луцюк О. О. Гібридні війни як інструмент міжнародної політики : робота на здобуття освіт. ступеня «Бакалавр» : спец. 052 «Політологія» / наук. кер. В. М. Пахолок ; Волин. нац. ун-т ім. Лесі Українки. Луцьк, 2025. 45 с. URL: https://evnuir.vnu.edu.ua/bitstream/123456789/28295/1/Lutsiyk_2025.pdf (дата звернення: 05.11.2025).

61. Мінветеранів буде протидіяти гібридним фейкам про захисників, – Юлія Лапутіна на презентації книги «Стратегічні комунікації в умовах гібридної війни» / Міністерство у справах ветеранів України. 2021. 2 листоп. URL: https://mva.gov.ua/ua/news/minveteraniv-bude-protidiyati-gibridnim-fejkam-pro-zahisnikiv-yuliya-laputina-na-prezentaciyi-knigi-strategichni-komunikaciyi-v-umovah-gibridnoyi-vijni (дата звернення: 05.11.2025).

62. Побороти ворожу брехню: Центр протидії дезінформації працює вже понад 4 роки. *Рада національної безпеки і оборони України*. URL: https://www.rnbo.gov.ua/ua/Diialnist/7169.html (дата звернення: 05.11.2025).

63. Рекомендації та кращі кейси реалізації стратегічних комунікацій в умовах війни : практичний довідник / В. Азарова та ін. ; за заг. ред. Л. Компанцевої. Київ : 7БЦ, 2023. 232 с. URL: https://kharkivoda.gov.ua/content/documents/1260/125978/files/p_157_22537512.pdf (дата звернення: 06.11.2025).

64. Стратегічні комунікації у США: 80% реальних дій і лише 20% слів. *Детектор медіа*. 2017. 13 жовт. URL: https://detector.media/infospace/article/130925/2017-10-13-strategichni-komunikatsii-u-ssha-80-realnykh-diy-i-lyshe-

20-sliv/ (дата звернення: 06.11.2025).

65. Стратегічні комунікації у фокусі співробітництва Україна–ЄС–НАТО в сучасних умовах / Центр глобалістики «Стратегія XXI». 2024. 05 лип. URL: https://geostrategy.org.ua/analityka/analitychna-zapyska/strategichni-komunikaciyi-u-fokusi-spivrobitnyctva-ukrayina-yes-nato-v-suchasnyh-umovah/823 (дата звернення: 06.11.2025).

66. Тихомирова Є. Б. Стратегічні комунікації як один з пріоритетів глобальної стратегії зовнішньої політики і безпеки ЄС. *Міжнародні відносини. Серія : Політичні науки*. 2017. № 14. URL: https://core.ac.uk/download/pdf/153587132.pdf (дата звернення: 05.11.2025).

67. Уздєнова Ю. М. Гібридна війна: сутність, складові та ключові поняття. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Державне управління*. 2024. Т. 35 (74), № 4. С. 26–30. DOI: https://doi.org/10.32782/TNU-2663-6468/2024.4/26.

68. Хагельстам А. Співпраця заради протидії гібридним загрозам. *NATO Review*. 2018. 23 листоп. URL: https://www.nato.int/docu/review/uk/articles/2018/11/23/spvpratsya-zaradi-protid-gbridnim-zagrozam/index.html (дата звернення: 05.11.2025).

69. Центр протидії дезінформації. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BD%D1%82%D1%80_%D0%BF%D1%80%D0%BE%D1%82%D0%B8%D0%B4%D1%96%D1%97_%D0%B4%D0%B5%D0%B7%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97 (дата звернення: 05.11.2025).

70. Юськів Б., Карпчук Н., Пелех О. Структура стратегічних комунікацій як основа ефективного комунікаційного менеджменту України в умовах війни. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2023. № 2 (16). С. 92–118. DOI: https://doi.org/10.29038/2524-2679-2023-02-92-118.