Харківський національний університет імені В.Н. Каразіна
Навчально-науковий інститут «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Кафедра міжнародних відносин

КВАЛІФІКАЦІЙНА

РОБОТА МАГІСТРА

на тему: **«НАТО у забезпеченні інформаційної безпеки в умовах гібридних загроз»**

Виконав:
студент 2-го курсу, групи УМІБ-61
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
ОПП «Міжнародна інформаційна безпека»
Котляров Максим Артемович
(прізвище, ім'я, по батькові)

Керівник:
Солових Віталій Павлович., д.держ.упр.,проф.
(науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

Рецензент:
к. соц. н., доцент Зінчина Олександра Борисівна
(науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

ХАРКІВ - 2025 р.

Харківський національний університет імені В. Н. Каразіна
Навчально-науковий інститут «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Кафедра міжнародних відносин
Спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
Освітньо-професійна програма «Міжнародна інформаційна безпека»
Рівень вищої освіти: другий (магістерський)

ЗАТВЕРДЖУЮ
завідувач кафедри

_____
(Підпис)

Наталія ВІННИКОВА
(ім'я, прізвище)

«2» червня 2025 року
(зі змінами від 10.09.2025; 06.10.2025)

ЗАВДАННЯ
на кваліфікаційну роботу магістра

Котлярова Максима Артемовича
(прізвище, ім'я та по батькові)
Тема роботи «НАТО у забезпеченні інформаційної безпеки в умовах гібридних загроз»

керівник роботи Солових Віталій Павлович., д.держ.упр.,проф.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом по університету від «02» червня 2025 року № 4001-5/1324 зі змінами від «10» вересня 2025 року № 4001-5/3049, зі змінами від «6» жовтня 2025 року № 4001-5/3656.

2. Строк подання здобувачем вищої освіти роботи 21 листопада 2025 р.
3. Перелік питань, які потрібно розробити:
Розкрити теоретичні концепції, що формують основу діяльності НАТО у сфері інформаційної безпеки; з'ясувати хід еволюції теоретичних підходів НАТО до інформаційної безпеки в контексті гібридних загроз; виокремити ключові доктрини НАТО та їх роль у протидії гібридним загрозам в інформаційному просторі; встановити роль НАТО у протидії російській дезінформації проти України з 2014 року; встановити способи заходів НАТО з інформаційної безпеки в умовах кібератак;

4. План роботи

№ з/п	Назви етапів роботи	Строк виконання етапів
1	Вибір здобувачем теми КРМ і подання заяви на кафедру; затвердження теми та призначення наукового керівника; складання та затвердження індивідуального завдання на виконання КРМ	12.05.2025-30.06.20255
2	Підготовка вступу і розділу 1 КРМ	22.09.2025-30.09.2025
3	Підготовка розділу 2 КРМ	01.10.2025-15.10.2025
4	Підготовка розділу 3 КРМ	16.10.2025-31.10.2025
5	Підготовка висновків і переліку використаних джерел	03.11.2025-14.11.2025
6	Подання студентом завершеної КРМ науковому керівнику для перевірки та оформлення відгуку, перевірка КРМ на відсутність запозичень	17.11.2025-21.11.2025
7	Попередній розгляд КРМ на комісії від кафедри	24.11.2025-28.11.2025
8	Прийняття кафедрою рішення про допуск роботи до захисту в ЕК, оформлення та зовнішнє рецензування	01.12.2025-05.12.2025
9	Захист КРМ в ЕК і присвоєння випускникам кваліфікації	08.12.2025-24.12.2025

5. Дата видачі завдання: 2 червня 2025 року (зі змінами від 10.09.2025; 06.10.2025).

Здобувач вищої освіти _____ Максим Котляров
(підпис) (ім'я, прізвище)

Керівник роботи _____ Віталій Солових
(підпис) (ім'я, прізвище)

ЗМІСТ

ВСТУП

Актуальність теми - У сучасному світі, де гібридні загрози поєднують військові, економічні, інформаційні та кібернетичні методи, інформаційна безпека стала ключовим елементом національної та міжнародної стабільності. Розвиток цифрових технологій, зокрема соціальних мереж, штучного інтелекту та кібероперацій, радикально змінив природу конфліктів, зробивши інформаційний простір ареною боротьби за вплив на суспільну свідомість і стратегічні рішення.

Ступінь дослідженності теми - тема НАТО в забезпеченні інформаційної безпеки в умовах гібридних загроз ґрунтовно розроблена у зарубіжній та вітчизняній літературі.

За кордоном ключовий внесок зробили: Atlantic Council, Brookings Institution, NATO StratCom COE, NATO CCDCOE, Hybrid CoE , автори Frontiers in Big Data, Center for European Policy Analysis, German Marshall Fund та Texas National Security Review.

В Україні тему досліджують Рада національної безпеки і оборони, Центр стратегічних комунікацій та інформаційної безпеки при МКІП, експерти Міноборони.

Мета дослідження - визначити роль НАТО у забезпеченні інформаційної безпеки в умовах гібридних загроз.

На основі визначеної мети дослідження виділено **такі завдання**:

- розкрити теоретичні концепції, що формують основу діяльності НАТО у сфері інформаційної безпеки;

- з’ясувати хід еволюції теоретичних підходів НАТО до інформаційної безпеки в контексті гібридних загроз;

- виокремити ключові доктрини НАТО та їх роль у протидії гібридним загрозам в інформаційному просторі;

- встановити роль НАТО у протидії російській дезінформації проти України з 2014 року; встановити способи заходів НАТО з інформаційної безпеки в умовах кібератак;

- запропонувати рекомендації для посилення ролі НАТО у протидії гібридним загрозам на основі аналізу кейсів втручання у вибори після 2016 року.

Об'єкт дослідження - НАТО, як актор у забезпеченні інформаційної безпеки в цифровому світі.

Предмет дослідження - діяльність НАТО у протидії гібридним інформаційним загрозам у сучасних конфліктах.

Методи дослідження.

- Системний аналіз - використаний для розгляду НАТО як цілісної системи, що включає політичні, військові, комунікаційні та кібернетичні компоненти. Дозволив показати, як усі елементи Альянсу взаємодіють між собою і формують єдину систему протидії гібридним інформаційним загрозам.
- Структурно-функціональний метод - застосовано для аналізу внутрішньої структури ключових органів і документів НАТО та визначення, яку саме функцію кожен з них виконує у боротьбі з дезінформацією, когнітивною війною та кібератаками.
- Компаративний метод - використано для порівняння:

еволюції доктрин НАТО; підходів НАТО та ЄС до протидії дезінформації; російських інформаційних кампаній проти України та країн Балтії/Польщі/Чехії після 2016 року.

- Кейс-метод (аналіз конкретних випадків) - детально досліджено три ключові кейси:

1. російська дезінформація та історичні фейки проти України (2014-2025);
2. втручання у вибори та гібридні операції в країнах Балтії та Польщі (2016-2025);
3. кібератаки типу WhisperGate, NotPetya та операції проти критичної інфраструктури країн НАТО та України.

Практичне значення. Отримані результати мають високу ступінь готовності до впровадження на рівні стратегічних рекомендацій для НАТО та

України, з потенціалом масштабного використання в політиці безпеки Альянсу та партнерів.

Основні прикладні результати включають рекомендації щодо посилення ролі НАТО в протидії дезінформації та розробку спільних програм з Україною для моніторингу кібератак. Вони можуть бути впроваджені в галузях міжнародної безпеки, дипломатії та освіти, сприяючи вирішенню проблеми гібридних загроз шляхом підвищення стійкості суспільств, зменшення впливу російської пропаганди та посилення координації в реагуванні на когнітивні атаки, що в підсумку підвищить загальну стабільність євроатлантичного регіону.

Апробація. Апробація дипломної роботи пройшла у рамках круглого столу «Стратегічні напрями зовнішньої політики та дипломатії країн світу» «Роль НАТО у забезпеченні інформаційної безпеки в умовах гібридних загроз»

Структура роботи. Кваліфікаційна робота складається зі вступу, трьох розділів, висновків та списку використаних джерел, який налічує 64 найменування. Загальний обсяг роботи становить 89 сторінок, з яких основного тексту - 79 сторінок.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ РОЛІ НАТО В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

1.1. Концептуальні основи діяльності НАТО в інформаційній сфері

Інформаційна війна, як теоретична концепція, займає центральне місце в сучасних дослідженнях безпеки, відображаючи зростаючу роль інформаційного простору в міжнародних конфліктах. У діяльності НАТО вона розглядається як комплекс стратегій, спрямованих на контроль, маніпуляцію та захист інформації для забезпечення переваги над противником у когнітивній, політичній і суспільній сферах. Інформаційна війна охоплює використання дезінформації, пропаганди, кібероперацій та психологічних операцій (PSYOPS) для впливу на сприйняття цільової аудиторії. Для НАТО, яке функціонує в умовах гібридних загроз, ця концепція є основою для розробки механізмів захисту країн-членів і партнерів від маніпулятивних інформаційних кампаній, що загрожують стабільності та безпеці. Особливо після 2014 року, коли російська агресія проти України виявила нові виклики в інформаційному просторі, Альянс переосмислив інформаційну війну як ключовий елемент гібридного конфлікту, де інформація виступає інструментом дестабілізації суспільств і держав.

Концепція інформаційного домінування є основоположною в теорії інформаційної війни, передбачаючи контроль над інформаційними потоками для впливу на рішення на індивідуальному, суспільному та державному рівнях. Ця ідея, сформована в західних військових доктринах наприкінці XX століття, була адаптована НАТО для протидії сучасним загрозам [1]. У контексті гібридних конфліктів інформаційне домінування дозволяє нейтралізувати ворожі наративи та просувати власні повідомлення. Наприклад, під час анексії Криму в 2014 році Росія використовувала дезінформацію про "нелегітимність" української влади, що ускладнювало консолідацію міжнародної підтримки України. НАТО, у відповідь, почало розробляти стратегії для протидії таким кампаніям, акцентуючи на швидкому реагуванні та координації між країнами-членами для забезпечення єдиного інформаційного фронту. Цей підхід

демонструє, як інформаційна війна трансформується в інструмент геополітичного впливу, що вимагає від Альянсу гнучкості та адаптивності.

Кібероперації є ще одним ключовим елементом теорії інформаційної війни, інтегруючись із дезінформаційними кампаніями для посилення їхнього ефекту. Кібератаки на критичну інфраструктуру чи інформаційні системи часто супроводжуються пропагандою для створення паніки та хаосу. Для НАТО цей аспект набув особливого значення після кібератак на Естонію в 2007 році та Україну в 2015-2016 роках, зокрема атаки на енергетичну систему України, що підкреслило необхідність визнання кіберпростору окремим доменом операцій [2]. Це відображає еволюцію теорії інформаційної війни, яка дедалі більше враховує технологічні виклики, пов’язані з цифровим середовищем. НАТО активно розвиває кіберзахист, інтегруючи його в ширшу стратегію інформаційної безпеки, що дозволяє протидіяти комбінованим загрозам, де інформаційні та кібернетичні атаки діють синергетично.

Ще одним важливим аспектом інформаційної війни є використання соціальних мереж як каналу для швидкого поширення маніпулятивного контенту. З 2014 року противники НАТО, зокрема Росія, активно застосовували платформи, такі як Twitter (тепер X) і Telegram, для просування наративів, що підривають довіру до Альянсу. Наприклад, у Балтійському регіоні російські кампанії націлювалися на російськомовне населення, просуваючи ідеї про "агресивність НАТО" та "утиски меншин", що створювало напругу в суспільствах країн-членів [3]. У відповідь НАТО розробило механізми стратегічних комунікацій, які передбачають моніторинг інформаційного простору та швидке реагування на дезінформацію, що дозволяє мінімізувати вплив таких кампаній.

У майбутньому, до 2026-2029 років, теорія інформаційної війни ймовірно враховуватиме зростаючу роль штучного інтелекту та автоматизованих систем у створенні дезінформації, таких як глибокі фейки. Для НАТО це означатиме потребу в нових теоретичних моделях, які б ураховували швидкість і точність сучасних інформаційних загроз, а також способи захисту

суспільної свідомості від маніпуляцій, що тісно пов’язане з концепцією когнітивної безпеки. Такі моделі можуть включати розвиток алгоритмів для виявлення автоматизованих кампаній, де ШІ аналізує патерни поведінки в соціальних мережах, передбачаючи поширення фейкових наративів ще на ранніх етапах. Наприклад, у сценаріях, подібних до російських операцій проти України, НАТО міг би використовувати ШІ для симуляції потенційних інформаційних атак, оцінюючи їхній вплив на суспільну думку в країнах-членах, таких як Польща чи Литва. Це дозволило б заздалегідь готувати контрзаходи, включаючи освітні програми з медіаграмотності, адаптовані до локальних культурних контекстів.

Крім того, еволюція теорії інформаційної війни в майбутньому може передбачати інтеграцію біометричних даних і нейротехнологій для більш точного таргетингу аудиторії. Для НАТО це створює як можливості, так і ризики, оскільки противники можуть використовувати ці технології для персоналізованих психологічних атак, що впливають на емоційний стан індивідів через персоналізований контент. Альянс, у свою чергу, міг би розвивати етичні рамки для використання таких технологій у оборонних цілях, наприклад, для моніторингу інформаційного поля в реальному часі і швидкого реагування на загрози. Аналіз поточних тенденцій, таких як використання ШІ в дезінформаційних кампаніях під час виборів у країнах НАТО в 2024 році, показує, як ці технології можуть посилювати поляризацію суспільства, що вимагає від Альянсу інноваційних підходів до теоретичного моделювання [4].

Прогнози щодо 2026-2029 років також вказують на потенційне зростання ролі віртуальної та доповненої реальності в інформаційних війнах, де фейкові події можуть бути візуалізовані для посилення емоційного впливу. Для НАТО це означатиме необхідність розширення теоретичних рамок для включення цих елементів, розробляючи стратегії, які поєднують технічні інструменти з психологічним аналізом для захисту когнітивної сфери. Такі зміни підкреслюють, як теорія інформаційної війни стає все більш

багатошаровою, інтегруючи елементи когнітивної безпеки для забезпечення довгострокової стійкості до гібридних загроз.

Теорія інформаційної війни також враховує економічний вимір, де дезінформація може бути використана для впливу на фінансові ринки та економічну стабільність країн. Для НАТО це означає розробку стратегій, які захищають критичні економічні сектори від інформаційних атак, таких як фейкові новини про фінансові кризи чи санкції. Наприклад, у контексті російських кампаній проти України, дезінформація про "економічний колапс" мала на меті підірвати довіру інвесторів, що вимагало від Альянсу координації з економічними інституціями для стабілізації ситуації. У майбутньому, з інтеграцією блокчейн-технологій і криптовалют, інформаційна війна може еволюціонувати до форм, де маніпуляції з даними впливають на глобальні фінансові потоки, що потребує від НАТО нових теоретичних підходів до захисту економічної когнітивної сфери [5].

Аналізуючи роль даних у теорії інформаційної війни, варто відзначити, як великі дані (big data) стають інструментом для прогнозування суспільних реакцій. Для НАТО це відкриває можливості для превентивних заходів, де аналіз даних дозволяє передбачати інформаційні атаки та готувати відповіді. Наприклад, під час ескалації в Україні в 2022 році, НАТО використовувало дані з відкритих джерел для моніторингу російських наративів, що дозволило швидко нейтралізувати їх через міжнародні комунікації. У прогнозах на 2026-2029 роки, з розвитком квантових обчислень, теорія може включати моделі, де обробка даних відбувається на безпрецедентному рівні, дозволяючи противникам створювати надточні маніпуляції, що вимагає від Альянсу інвестицій у технології захисту даних і когнітивної безпеки.

Концепція гібридних загроз стала однією з ключових парадигм у сучасних дослідженнях міжнародної безпеки, відображаючи еволюцію конфліктів від традиційних війн до складних, багатошарових форм протистояння, де військові дії поєднуються з інформаційними, економічними, політичними та кібернетичними інструментами. У контексті діяльності НАТО

гібридні загрози визначаються як стратегії, що використовуються державами або недержавними акторами для досягнення стратегічних цілей через комбінацію відкритих і прихованих операцій, спрямованих на дестабілізацію супротивника без повномасштабної війни. Ці загрози розмивають межі між війною і миром, створюючи "сіру зону", де традиційні підходи до безпеки, такі як військові альянси та договори, стають менш ефективними через їхню нездатність повністю охопити неконвенційні методи впливу. Для НАТО, як трансатлантичного альянсу, що зіштовхується з викликами від авторитарних режимів, таких як Росія, концепція гібридних загроз є фундаментальною для розуміння сучасних геополітичних реалій і розробки відповідних стратегій протидії. Інтеграція інформаційних методів, таких як дезінформація, пропаганда і психологічні операції, з традиційними формами впливу, такими як військові дії, економічний тиск чи дипломатичний шантаж, становить основу цієї концепції, що вимагає від Альянсу комплексного, мультидисциплінарного підходу до забезпечення колективної безпеки.

Історично концепція гібридних загроз виникла в контексті пост-холодновійнної ери, коли традиційні симетричні конфлікти поступилися місцем асиметричним формам протистояння, де слабші актори могли ефективно протистояти сильнішим через використання неконвенційних методів. У 2000-х роках терміни "гібридна війна" та "нелінійна війна" почали використовуватися в західних військових доктринах, але справжнього розголосу вони набули після 2014 року, коли Росія застосувала комбінацію військових, інформаційних і економічних засобів для анексії Криму та дестабілізації східних регіонів України. Цей підхід, часто асоційований із так званою "доктриною Герасимова", опублікованою в 2013 році, підкреслює перевагу несилових методів, таких як інформаційні операції, над традиційними військовими діями у співвідношенні 4:1 [5]. У російсько-українському конфлікті інформаційні методи стали основним інструментом для підготовки ґрунту до військових операцій, дозволяючи Росії досягати цілей з мінімальними витратами ресурсів і уникати прямого протистояння з НАТО. Наприклад, перед

анексією Криму Росія активно використовувала дезінформаційні кампанії, поширюючи через державні медіа, такі як RT і Sputnik, наративи про "геноцид російськомовного населення" та "нелегітимність" української влади після Майдану. Ці наративи не лише виправдовували військову інтервенцію, але й створювали сприятливе інформаційне середовище, що дозволяло Росії діяти швидко та ефективно, демонструючи, як інформаційні методи інтегруються з традиційними військовими операціями для створення ефекту сюрпризу та дезорієнтації супротивника.

Інформаційні операції в рамках гібридних загроз характеризуються системним використанням дезінформації для маніпуляції суспільною свідомістю, що є одним з найбільш ефективних способів підриву стабільності без прямого застосування сили. У 2014 році Росія застосовувала соціальні мережі, такі як VKontakte і Telegram, для швидкого поширення фейкових новин, які підривали довіру до української влади та мобілізували підтримку серед місцевого населення. Наприклад, історія про "розп’ятого хлопчика" на Донбасі, поширена російськими медіа, мала на меті викликати емоційний резонанс і виправдати підтримку сепаратистських рухів, створюючи ілюзію гуманітарної кризи [6]. Ці дії ілюструють, як гібридні загрози використовують психологічний вплив для посилення ефективності інформаційних кампаній, апелюючи до емоцій, страхів і культурних упереджень аудиторії. Для НАТО це створює необхідність розробки механізмів швидкого реагування, які дозволяють виявляти та нейтралізувати дезінформацію на ранніх етапах її поширення. Альянс активно працює над створенням інструментів моніторингу інформаційного простору, що включають аналіз соціальних мереж і співпрацю з технологічними компаніями для виявлення фейкових акаунтів і ботів, які ампліфікують маніпулятивний контент. Такий підхід не лише допомагає захищати країни-члени, але й дозволяє Альянсу просувати власні наративи, що підкреслюють цінності демократії та солідарності.

Кібернетичні операції є невід’ємною частиною гібридних загроз, інтегруючись із інформаційними методами для посилення їхнього впливу і

створення синергетичного ефекту. Кібератаки на критичну інфраструктуру, такі як енергетичні системи, урядові мережі чи фінансові установи, часто супроводжуються дезінформаційними кампаніями для створення паніки, хаосу та псування репутації супротивника. У 2015-2016 роках Україна зазнала серії кібератак, зокрема на енергетичну систему, які поєднувалися з інформаційними кампаніями, що звинувачували український уряд у "некомпетентності" і "відсутності контролю". Ці атаки підкреслили важливість кіберпростору як домену гібридного конфлікту, що змусило НАТО визнати його окремим операційним простором у 2016 році на Варшавському саміті [3]. Для Альянсу це означало необхідність розвитку інтегрованих стратегій, які поєднують кіберзахист із протидією дезінформації, щоб забезпечити комплексний захист від гібридних загроз. Наприклад, у Балтійському регіоні НАТО проводить регулярні кібернавчання, такі як Cyber Coalition, для підвищення готовності країн-членів до таких атак, симулюючи сценарії, де кібератаки поєднуються з інформаційними кампаніями для перевірки реакції та координації. Ці навчання не лише покращують технічну готовність, але й розвивають психологічну стійкість, навчаючи учасників розпізнавати та реагувати на маніпулятивний контент, що супроводжує кібератаки.

Економічний тиск є ще одним ключовим елементом гібридних загроз, який використовується для посилення інформаційних і військових операцій, створюючи довгостроковий ефект на супротивника. У контексті російсько-українського конфлікту Росія застосовувала економічні інструменти, такі як обмеження постачання газу, торговельні санкції чи маніпуляції з валютними ринками, паралельно з інформаційними кампаніями, що просували ідею "економічного колапсу" України. Ці дії мали на меті підірвати довіру до української економіки, послабити її позиції на міжнародній арені та створити внутрішній хаос, що полегшувало військові операції. Для НАТО протидія таким загрозам вимагає не лише інформаційних, але й економічних стратегій, які включають співпрацю з фінансовими інституціями для стабілізації економік країн-партнерів. Наприклад, Альянс підтримує програми економічної стійкості

в Україні, що включають консультації з питань енергетичної безпеки, диверсифікації економічних ресурсів і захисту від економічного шантажу. Ці програми не лише допомагають Україні, але й служать моделлю для інших країн, таких як Молдова чи Грузія, які можуть стати цілями подібних гібридних атак.

Дипломатичні та політичні інструменти також відіграють значну роль у гібридних загрозах, посилюючи інформаційні операції через міжнародні платформи. У 2014-2015 роках Росія активно просувала свої наративи через міжнародні організації, такі як ООН і ОБСЄ, намагаючись легітимізувати анексію Криму, паралельно використовуючи дезінформацію для дискредитації України на глобальному рівні. Для НАТО це створює виклик у сфері стратегічних комунікацій, оскільки Альянс мусить не лише протидіяти дезінформації, але й формувати власні наративи для підтримки міжнародної єдності та ізоляції агресора. Наприклад, після 2014 року НАТО посилило свою присутність у Балтійському регіоні, використовуючи інформаційні кампанії для демонстрації солідарності з країнами-членами, такими як Естонія та Латвія, які зазнали дипломатичного тиску з боку Росії [3]. Ці зусилля включають регулярні дипломатичні консультації, спільні декларації та медійні кампанії, що підкреслюють колективну оборону і стримують потенційних агресорів.

Соціокультурний аспект гібридних загроз є особливо важливим, оскільки противники використовують історичні, культурні та етнічні наративи для розколу суспільства і послаблення внутрішньої єдності. У російсько-українському конфлікті Росія просувала ідеї "русского мира", апелюючи до історичних і культурних зв’язків, щоб виправдати свою агресію та мобілізувати підтримку серед російськомовного населення. Для НАТО це створює необхідність розробки контрнаративів, які підкреслюють демократичні цінності, толерантність і єдність країн-членів. У Польщі та Литві Альянс підтримує програми, спрямовані на інтеграцію меншин і протидію маніпулятивним наративам, що мають на меті послабити соціальну згуртованість. Ці програми включають освітні ініціативи з медіаграмотності,

культурні обміни та громадські кампанії, які допомагають населенню розпізнавати дезінформацію та протистояти їй, сприяючи довгостроковій стійкості суспільства до гібридних загроз[7]

Прогнозуючи розвиток гібридних загроз до 2026-2029 років, можна очікувати значного зростання їхньої складності за рахунок використання штучного інтелекту (ШІ) і технологій глибоких фейків. ШІ дозволяє створювати персоналізовані дезінформаційні кампанії, які адаптуються до індивідуальних уподобань аудиторії, роблячи їх більш ефективними та важко виявленими. У 2024 році було зафіксовано спроби використання ШІ для створення фейкових відеороликів, які дискредитували політичних лідерів у країнах НАТО, що підкреслює необхідність для Альянсу розвитку нових стратегій. Наприклад, НАТО може впроваджувати системи аналізу великих даних для моніторингу інформаційного простору, що дозволить виявляти аномалії в поширенні контенту та передбачати дезінформаційні кампанії. Крім того, Альянс може співпрацювати з приватними компаніями, такими як Google чи Meta, для створення інструментів, які автоматично маркують фейковий контент, допомагаючи користувачам розпізнавати маніпуляції.

Іншим напрямом розвитку гібридних загроз є використання віртуальної та доповненої реальності для створення переконливих фейкових подій. У майбутньому противники можуть створювати віртуальні сценарії, які імітують реальні конфлікти чи катастрофи, щоб викликати паніку або політичну нестабільність. Для НАТО це означатиме необхідність розробки нових теоретичних моделей, які враховують ці технології, а також співпраці з технологічними компаніями для створення інструментів моніторингу таких загроз. Наприклад, у Балтійському регіоні, де Росія активно використовує інформаційні кампанії, НАТО може впроваджувати симуляційні програми для прогнозування впливу таких технологій на суспільство, щоб заздалегідь готувати контрзаходи, включаючи освітні кампанії та технічні фільтри для віртуальної реальності[7].

Економічний вимір гібридних загроз набуває нових форм із поширенням криптовалют і блокчейн-технологій, які дозволяють противникам фінансувати дезінформаційні кампанії анонімно. У 2023 році було зафіксовано спроби використання криптовалют для фінансування пропагандистських кампаній, спрямованих проти України, що підкреслює необхідність для НАТО розробки стратегій захисту фінансового сектора [8]. У майбутньому ці загрози можуть стати більш складними, що вимагатиме від Альянсу інтеграції економічної безпеки в ширшу стратегію протидії гібридним загрозам. Наприклад, НАТО може співпрацювати з міжнародними фінансовими організаціями для створення механізмів моніторингу транзакцій, які можуть бути пов'язані з гібридними операціями, а також розвивати програми для підвищення фінансової грамотності серед населення, щоб зменшити вразливість до економічних маніпуляцій.

Біотехнології також можуть стати частиною гібридних загроз, оскільки противники можуть використовувати аналіз біометричних даних для створення персоналізованих інформаційних атак. Такі атаки можуть враховувати фізіологічні реакції аудиторії, роблячи їх більш ефективними. Для НАТО це означатиме необхідність розробки етичних рамок для захисту від таких загроз, а також інтеграції біотехнологій у стратегії інформаційної безпеки. Наприклад, Альянс може розробляти системи для захисту особистих даних громадян країн-членів, щоб запобігти їх використанню в маніпулятивних кампаніях. Аналіз поточних тенденцій, таких як використання ШІ для аналізу біометричних даних, показує, що противники вже експериментують із такими технологіями, що вимагає від НАТО інноваційних підходів до захисту[9].

У довгостроковій перспективі гібридні загрози можуть включати використання квантових обчислень для аналізу великих даних і створення складних моделей маніпуляцій. Для НАТО це означатиме необхідність інвестувати в нові технології, які дозволяють виявляти та нейтралізувати такі загрози, а також розвивати міждисциплінарні підходи, що поєднують інформаційні, економічні та соціокультурні стратегії. Наприклад, Альянс може

створювати спеціалізовані центри для аналізу квантових загроз, які поєднують експертизу в технологіях і соціальних науках. Такі центри могли б прогнозувати потенційні сценарії гібридних атак, що включають комбінацію квантових обчислень і дезінформації, щоб заздалегідь розробляти контрзаходи.

Крім того, гібридні загрози можуть еволюціонувати до форм, де екологічні фактори використовуються як інструмент впливу. Противники можуть маніпулювати інформацією про екологічні катастрофи, щоб створити паніку або політичну нестабільність. Для НАТО це означатиме необхідність включення екологічної безпеки в стратегію протидії, розробляючи програми для моніторингу екологічних наративів і захисту критичної екологічної інфраструктури. Наприклад, у контексті змін клімату Альянс може проводити спільні навчання для реагування на комбіновані загрози, де дезінформація про екологічні проблеми поєднується з кібератаками на екологічні системи[10].

Соціальні мережі залишатимуться ключовим полем для гібридних загроз, де противники використовують алгоритми для ампліфікації маніпулятивного контенту. У 2025 році тенденції показують, що ШІ-генерований контент стає все більш поширеним, що вимагає від НАТО розвитку інструментів для виявлення такого контенту. Альянс може співпрацювати з платформами для впровадження маркування ШІ-генерованого контенту, що допоможе користувачам розпізнавати фейки. Крім того, освітні програми з медіаграмотності можуть бути розширені для охоплення молодого покоління, яке є найбільш вразливим до таких загроз[11].

Когнітивна безпека є відносно новою, але критично важливою концепцією в теорії інформаційної війни, що зосереджується на захисті суспільної свідомості від маніпулятивних впливів, які мають на меті змінити сприйняття, поведінку та прийняття рішень як на індивідуальному, так і на суспільному рівнях. У контексті діяльності НАТО когнітивна безпека розглядається як ключовий елемент протидії гібридним загрозам, де дезінформація, пропаганда та психологічні операції використовуються для підриву довіри до демократичних інститутів, послаблення соціальної

згуртованості та дестабілізації держав. Ця концепція набуває особливого значення в епоху цифрових технологій, коли соціальні мережі, алгоритми штучного інтелекту (ШІ) та автоматизовані системи дозволяють противникам створювати високоточні маніпулятивні кампанії. Для НАТО, яке прагне забезпечити стійкість країн-членів і партнерів до таких загроз, когнітивна безпека є не лише реактивним механізмом захисту, але й проактивним інструментом для зміцнення суспільної свідомості через освіту, стратегічні комунікації та технологічні інновації. Зокрема, після 2014 року, коли російська агресія проти України продемонструвала ефективність інформаційних маніпуляцій, Альянс почав активно розвивати теоретичні моделі когнітивної безпеки, які поєднують психологічні, соціальні та технологічні підходи[12]

Теоретичні моделі когнітивної безпеки базуються на розумінні когнітивних процесів, які визначають, як люди сприймають, обробляють і реагують на інформацію. Однією з основних моделей є концепція когнітивних упереджень, яка пояснює, як людська свідомість схильна до спрощень і помилок у судженнях, що робить її вразливою до маніпуляцій. Наприклад, ефект підтвердження, коли люди схильні вірити інформації, яка відповідає їхнім наявним переконанням, активно використовується в дезінформаційних кампаніях. У російсько-українському конфлікті Росія застосовувала цю модель, поширюючи наративи про "нацистський уряд" у Києві, які знаходили відгук серед аудиторій, що вже мали упередження проти України [13]. Для НАТО протидія таким маніпуляціям передбачає розробку стратегій, які враховують когнітивні упередження, зокрема через просування альтернативних наративів, що ґрунтуються на фактах і апелюють до раціонального мислення. Ці стратегії включають освітні програми з медіаграмотності, які допомагають населенню розпізнавати маніпулятивний контент і критично оцінювати інформацію.

Ще однією важливою теоретичною моделлю є концепція когнітивного захисту, яка зосереджується на створенні психологічних і соціальних бар’єрів для маніпулятивного впливу. Ця модель передбачає використання стратегічних комунікацій для формування позитивних наративів, які зміцнюють довіру до

державних інститутів і демократичних цінностей. У контексті гібридних загроз НАТО застосовує цю модель для протидії дезінформаційним кампаніям, які мають на меті розкол суспільства. Наприклад, у Балтійському регіоні після 2014 року Росія використовувала наративи про "утиски російськомовного населення" в Естонії та Латвії, щоб посіяти недовіру до місцевих урядів і Альянсу[3]. У відповідь НАТО розробило програми стратегічних комунікацій, які підкреслюють єдність і безпеку країн-членів, а також підтримують ініціативи з інтеграції меншин, щоб зменшити вразливість до маніпуляцій. Ці програми включають створення контенту, який апелює до спільних цінностей, таких як свобода і демократія, що допомагає зміцнити когнітивну стійкість суспільства.

Технологічний аспект когнітивної безпеки є ще одним ключовим елементом, який набуває дедалі більшого значення в умовах цифрової епохи. Сучасні технології, такі як ШІ та аналіз великих даних, дозволяють противникам створювати персоналізовані дезінформаційні кампанії, які враховують індивідуальні вподобання та поведінку користувачів. У 2024 році, наприклад, було зафіксовано випадки використання ШІ для створення глибоких фейків, які дискредитували політичних лідерів у країнах НАТО, що підкреслює необхідність розвитку технологічних рішень для захисту когнітивного простору [14]. Для НАТО це означає необхідність інвестувати в технології, які дозволяють виявляти та нейтралізувати такі загрози, наприклад, системи аналізу даних для моніторингу соціальних мереж і виявлення аномалій у поширенні контенту. Крім того, Альянс може співпрацювати з технологічними компаніями для впровадження інструментів, які маркують ШІ-генерований контент, допомагаючи користувачам розпізнавати маніпуляції.

Іншим важливим аспектом когнітивної безпеки є захист від психологічних операцій (PSYOPS), які використовуються для маніпуляції емоційним станом аудиторії. Теоретичні моделі PSYOPS, що застосовуються в гібридних загрозах, базуються на принципах емоційного впливу, таких як страх, гнів чи гордість, які посилюють сприйнятливість до дезінформації. У

російсько-українському конфлікті Росія використовувала емоційно заряджені наративи, такі як історії про "гуманітарну кризу" на Донбасі, щоб мобілізувати підтримку серед населення та виправдати свою агресію [8]. Для НАТО протидія таким операціям передбачає розробку контрнаративів, які нейтралізують емоційний вплив і пропонують раціональні альтернативи. Наприклад, Альянс може створювати інформаційні кампанії, які підкреслюють факти і спростовують фейки, використовуючи при цьому емоційно нейтральний тон, щоб уникнути подальшої поляризації суспільства.

Соціокультурний вимір когнітивної безпеки також відіграє важливу роль, оскільки противники використовують культурні та історичні наративи для розколу суспільства. У контексті гібридних загроз Росія часто апелює до історичних зв’язків, таких як концепція "русского мира", щоб виправдати свої дії та послабити єдність країн, таких як Україна чи країни Балтії. Для НАТО це створює необхідність розробки стратегій, які враховують соціокультурні особливості аудиторії, щоб зміцнити соціальну згуртованість. Наприклад, у Польщі та Литві Альянс підтримує програми з інтеграції меншин, які включають культурні обміни та освітні ініціативи, спрямовані на протидію маніпулятивним наративам. Ці програми допомагають населенню розпізнавати дезінформацію, яка використовує культурні чи етнічні розбіжності, і сприяють формуванню спільної ідентичності, що ґрунтується на демократичних цінностях[7].

Прогнозуючи розвиток когнітивної безпеки до 2026-2029 років, можна очікувати, що гібридні загрози стануть ще більш складними за рахунок використання нейротехнологій і біометричних даних. Противники можуть застосовувати ці технології для аналізу фізіологічних реакцій аудиторії, створюючи персоналізовані маніпулятивні кампанії, які враховують емоційний стан і психологічні особливості індивідів. Для НАТО це означатиме необхідність розробки етичних рамок для захисту від таких загроз, а також інтеграції нейротехнологій у стратегії інформаційної безпеки. Наприклад, Альянс може створювати системи для захисту особистих даних громадян країн-

членів, щоб запобігти їх використанню в маніпулятивних кампаніях. Крім того, НАТО може інвестувати в дослідження нейрокогнітивних механізмів, щоб краще розуміти, як маніпуляції впливають на свідомість, і розробляти відповідні контрзаходи[15]

Економічний вимір когнітивної безпеки також набуває значення, оскільки дезінформація може впливати на фінансові ринки та економічну стабільність. У контексті російсько-українського конфлікту Росія використовувала наративи про "економічний колапс" України, щоб підірвати довіру інвесторів і послабити економіку країни. Для НАТО це підкреслює необхідність включення економічної безпеки в стратегії когнітивного захисту, наприклад, через співпрацю з фінансовими інституціями для стабілізації ринків і протидії маніпулятивним наративам. Альянс може також розвивати програми фінансової грамотності, які допомагають населенню розпізнавати дезінформацію, пов’язану з економічними питаннями[8]

Технологічний прогрес, зокрема використання квантових обчислень, може кардинально змінити підходи до когнітивної безпеки в майбутньому. Квантові обчислення дозволяють обробляти величезні обсяги даних із безпрецедентною швидкістю, що може бути використано противниками для створення складних моделей маніпуляцій. Для НАТО це означатиме необхідність інвестувати в подібні технології для прогнозування та нейтралізації таких загроз. Наприклад, Альянс може створювати спеціалізовані центри для аналізу квантових загроз, які поєднують експертизу в технологіях і соціальних науках, щоб розробляти моделі захисту від маніпулятивних кампаній.

Соціальні мережі залишатимуться ключовим полем для когнітивних атак, де алгоритми ШІ використовуються для ампліфікації маніпулятивного контенту. У 2025 році тенденції показують, що ШІ-генерований контент стає дедалі більш поширеним, що вимагає від НАТО розвитку інструментів для його виявлення. Альянс може співпрацювати з платформами, такими як Meta чи X, для впровадження маркування ШІ-генерованого контенту, що допоможе

користувачам розпізнавати фейки. Крім того, освітні програми з медіаграмотності можуть бути розширені для охоплення молодого покоління, яке є найбільш вразливим до таких загроз, через інтерактивні формати, такі як онлайн-курси чи гейміфіковані платформи.

Екологічний вимір когнітивної безпеки також може стати важливим у майбутньому, оскільки противники можуть маніпулювати інформацією про екологічні катастрофи, щоб викликати паніку або політичну нестабільність. Для НАТО це означатиме необхідність включення екологічної безпеки в стратегії когнітивного захисту, розробляючи програми для моніторингу екологічних наративів і захисту критичної інфраструктури. Наприклад, Альянс може проводити спільні навчання для реагування на комбіновані загрози, де дезінформація про екологічні проблеми поєднується з кібератаками на екологічні системи.

У довгостроковій перспективі когнітивна безпека вимагатиме від НАТО міждисциплінарного підходу, який поєднує психологічні, технологічні та соціокультурні стратегії. Альянс може створювати спеціалізовані центри для аналізу когнітивних загроз, які інтегрують експертизу в нейронауках, технологіях і соціальних науках. Ці центри могли б прогнозувати потенційні сценарії маніпулятивних кампаній, розробляючи контрзаходи, які враховують як індивідуальні, так і суспільні аспекти когнітивної безпеки[15].

1.2. Еволюція підходів НАТО до інформаційної безпеки

У період холодної війни (1947-1991) стратегії НАТО у сфері інформаційної безпеки формувалися в контексті глобального ідеологічного протистояння між Західним блоком і Радянським Союзом, де інформаційний простір відігравав ключову роль у боротьбі за вплив на суспільну свідомість. Основним завданням Альянсу було протидіяти радянській пропаганді, яка мала на меті підірвати єдність країн-членів НАТО, дискредитувати демократичні цінності та просувати комуністичну ідеологію. Інформаційна війна в той час

зосереджувалася на використанні традиційних медіа, таких як радіо, телебачення, преса та листівки, через які обидві сторони намагалися формувати сприйняття власних і ворожих дій.

Для НАТО інформаційна безпека була інструментом захисту від пропагандистських атак і засобом зміцнення єдності альянсу, що дозволяло підтримувати стратегічні цілі в умовах холодної війни. Цей період заклав основи для розуміння інформаційних операцій як частини ширшої стратегії безпеки, багато елементів якої можна порівняти з сучасними підходами до протидії гібридним загрозам, хоча сучасний цифровий контекст додав нових викликів і можливостей[16].

На початку холодної війни, після створення НАТО в 1949 році, інформаційні стратегії Альянсу були спрямовані на нейтралізацію радянських наративів, які зображали Захід як імперіалістичний блок, що загрожує миру. Радянський Союз через такі структури, як Комінформ, створений у 1947 році, координував пропагандистські кампанії, що просували ідею соціалістичного світу як альтернативи капіталістичному Заходу. Ці кампанії використовували радіомовлення, газети та культурні заходи для поширення наративів про "класову боротьбу" та "західний імперіалізм". У відповідь НАТО підтримувало ініціативи, такі як "Радіо Вільна Європа" та "Радіо Свобода", які транслювали програми для країн Східного блоку, акцентуючи на свободах, економічних можливостях і політичній стабільності Заходу. Ці радіостанції, хоча й фінансувалися переважно США, тісно співпрацювали з НАТО, щоб підірвати довіру до радянської системи [17]. Схожий підхід можна спостерігати в сучасних стратегіях НАТО, де Альянс використовує соціальні мережі та цифрові платформи для просування демократичних цінностей, наприклад, через кампанії, що спростовують дезінформацію про діяльність НАТО в Балтійському регіоні. Однак, якщо в холодну війну радіо було основним каналом, сучасний контекст вимагає роботи з динамічними цифровими платформами, що значно ускладнює завдання через швидкість і масштаби поширення інформації.

Інформаційні кампанії НАТО під час холодної війни також мали на меті створення позитивного іміджу Альянсу як захисника миру та стабільності. У 1950-х роках Альянс запустив низку ініціатив, таких як кампанія "Щит миру", яка використовувала плакати, документальні фільми та публікації для підкреслення ролі НАТО в запобіганні прямому військовому конфлікту з Радянським Союзом. Ці матеріали зображали НАТО як гаранта безпеки для Західної Європи, протиставляючи його радянській загрозі, яка часто асоціювалася з мілітаризацією та тоталітаризмом. Наприклад, у Західній Німеччині, де антивоєнні настрої могли послабити підтримку Альянсу, НАТО активно використовувало інформаційні матеріали для демонстрації переваг колективної оборони [18].

Сьогодні подібні стратегії можна побачити в інформаційних кампаніях НАТО, спрямованих на підтримку країн Балтії чи України, де Альянс використовує соціальні мережі для поширення повідомлень про солідарність і захист від зовнішніх загроз. Однак сучасні кампанії стикаються з викликом фрагментації аудиторії через різноманітність цифрових платформ, тоді як у холодну війну інформаційний простір був більш централізованим і передбачуваним.

Радянський Союз, зі свого боку, використовував широкий спектр пропагандистських методів, які включали не лише медіа, але й культурну дипломатію, таку як організація міжнародних фестивалів чи підтримка прокомуністичних рухів у Західній Європі. Наприклад, у 1960-х роках СРСР фінансував антивоєнні рухи в країнах НАТО, які звинувачували Альянс у провокуванні "ядерної гонки". Ці кампанії часто використовували емоційно заряджені наративи, щоб викликати страх і недовіру до НАТО серед населення країн-членів. У відповідь Альянс розробляв контрпропагандистські стратегії, які включали не лише спростування радянських наративів, але й просування позитивних історій про економічний і соціальний прогрес на Заході. Наприклад, НАТО підтримувало культурні обміни та виставки, які демонстрували переваги демократичного способу життя, такі як економічна

свобода та індивідуальні права [19]. Схожий підхід простежується в сучасних стратегіях Альянсу, де НАТО використовує стратегічні комунікації для просування демократичних цінностей у відповідь на дезінформаційні кампанії, наприклад, російські наративи про "агресивність НАТО". Однак сучасні кампанії вимагають швидшого реагування через миттєве поширення інформації в соціальних мережах, що контрастує з повільнішим темпом холодної війни.

Ще одним важливим аспектом інформаційної безпеки в період холодної війни було використання психологічних операцій (PSYOPS), які передбачали цілеспрямований вплив на суспільну свідомість через емоційні та ідеологічні меседжі. НАТО застосовувало PSYOPS для підтримки морального духу в країнах-членах і послаблення довіри до радянської системи в країнах Східного блоку. Наприклад, під час Берлінської кризи 1961 року Альянс використовував радіомовлення для передачі повідомлень до Східної Німеччини, які підкреслювали свободу Західного Берліна та контрастували її з обмеженнями радянського режиму. Ці операції були ретельно спланованими, щоб уникнути прямого провокування конфлікту, але водночас створювали психологічний тиск на СРСР [19]. У сучасному світі PSYOPS еволюціонували в складніші форми, такі як стратегічні комунікації, які використовують аналіз великих даних і соціальні мережі для таргетування аудиторій. Наприклад, сучасні кампанії НАТО в Балтійському регіоні спрямовані на протидію російським наративам через персоналізовані повідомлення в соціальних мережах, що враховують культурні та мовні особливості аудиторії. Однак, на відміну від холодної війни, сучасні PSYOPS стикаються з викликом дезінформації, яка поширюється через автоматизовані боти та ШІ, що вимагає нових технологічних рішень.

Кризові моменти холодної війни, такі як Карибська криза 1962 року, виявили обмеженість інформаційних стратегій того часу, коли швидкість реагування була ускладнена відсутністю цифрових технологій. Під час цієї кризи НАТО використовувало дипломатичні канали та обмежені медійні ресурси для донесення своєї позиції, але брак швидких каналів комунікації

ускладнював протидію радянським наративам, які звинувачували Захід у провокуванні конфлікту. У сучасних умовах НАТО має значно ширші можливості для швидкого реагування, наприклад, через соціальні мережі та міжнародні платформи, але стикається з проблемою інформаційного перевантаження, коли фейкові наративи можуть поширюватися швидше, ніж офіційні спростування. Ця різниця підкреслює, як холодна війна навчила НАТО важливості координації інформаційних зусиль, але сучасний контекст вимагає адаптації до нових технологічних реалій.

Інформаційна безпека в період холодної війни також включала захист від шпигунства та дезінформації, які використовувалися СРСР для впливу на внутрішню політику країн НАТО. Наприклад, КДБ проводило операції з дезінформації, такі як поширення фальшивих документів, які звинувачували Захід у плануванні агресії проти СРСР. НАТО, зі свого боку, створювало системи для виявлення таких операцій, включаючи співпрацю з національними розвідками для аналізу ворожих пропагандистських матеріалів. Цей досвід можна порівняти з сучасними зусиллями Альянсу з протидії дезінформації, наприклад, через Центр стратегічних комунікацій у Ризі, який аналізує російські наративи та розробляє контрзаходи. Однак, якщо в холодну війну дезінформація поширювалася повільно через фізичні носії, сучасні цифрові платформи дозволяють противникам діяти миттєво, що вимагає від НАТО нових інструментів, таких як алгоритми аналізу даних[20]

Іншим аспектом інформаційних стратегій НАТО було залучення громадської думки в країнах-членах для підтримки політики стримування. У 1970-х роках, коли Радянський Союз розгорнув ядерні ракети SS-20, НАТО зіткнулося з необхідністю переконати європейське населення в необхідності розміщення американських ракет Pershing II у відповідь. Для цього Альянс використовував інформаційні кампанії, які пояснювали загрозу радянської мілітаризації та підкреслювали важливість єдності НАТО. Ці кампанії включали публічні виступи, статті в пресі та документальні фільми, які апелювали до безпеки та миру.

Інформаційні стратегії НАТО в період холодної війни також включали співпрацю з союзниками для координації повідомлень. Наприклад, Альянс тісно співпрацював із США, Великою Британією та Францією для створення єдиного інформаційного фронту, який протидіяв радянським наративам. Ця співпраця включала обмін розвідданими про пропагандистські операції СРСР і розробку спільних медійних кампаній. Сучасні стратегії НАТО також спираються на співпрацю, але включають ширший спектр акторів, таких як технологічні компанії та неурядові організації, що допомагають у боротьбі з дезінформацією. Наприклад, співпраця з платформами, такими як Meta чи X, дозволяє Альянсу швидше виявляти та нейтралізувати фейкові акаунти, що використовуються для поширення маніпулятивного контенту.

Інформаційна безпека в період холодної війни була обмежена технологічними можливостями того часу, але заклала основи для розуміння важливості інформаційного простору в безпековій політиці. Досвід протидії радянській пропаганді, використання PSYOPS і координація з союзниками сформували підходи, які НАТО адаптувало до сучасних викликів. Хоча інструменти змінилися від радіо до соціальних мереж, основна мета залишилася незмінною: захист суспільної свідомості від маніпуляцій і зміцнення єдності Альянсу перед зовнішніми загрозами[20].

1.3. Доктринальні основи протидії гібридним загрозам

Стратегічна концепція НАТО 2022 року, ухвалена на Мадридському саміті, стала важливим кроком у розвитку підходів Альянсу до протидії гібридним загрозам, зокрема в контексті інформаційної безпеки. Цей документ відображає адаптацію НАТО до нових реалій глобального безпекового середовища, де інформаційний простір визнано ключовим доменом сучасних конфліктів. У відповідь на зростання гібридних загроз, таких як дезінформація, кібератаки та психологічні операції, Стратегічна концепція 2022 року вперше чітко артикулює інформаційну безпеку як невід’ємну частину колективної

оборони Альянсу. З урахуванням досвіду російської агресії проти України, яка посилила актуальність гібридних методів, документ визначає інформаційну безпеку як пріоритет, що охоплює захист суспільної свідомості, протидію дезінформації та зміцнення стійкості країн-членів і партнерів. У цьому контексті Стратегічна концепція 2022 року закладає доктринальні основи для інтеграції інформаційних і традиційних методів у стратегіях НАТО, підкреслюючи необхідність комплексного підходу до протидії маніпулятивним впливам[21].

Ключові положення щодо інформаційної безпеки:

1. Визнання інформаційного простору як домену операцій
Стратегічна концепція 2022 року офіційно визнає інформаційний простір одним із ключових доменів поряд із сушею, морем, повітрям і кіберпростором. Це відображає розуміння того, що маніпуляції в інформаційному середовищі можуть мати стратегічний ефект, порівнянний із традиційними військовими діями. Документ підкреслює, що дезінформація, пропаганда та психологічні операції, які використовуються державами чи недержавними акторами, можуть дестабілізувати суспільства, підірвати довіру до демократичних інститутів і послабити єдність Альянсу. Наприклад, російські дезінформаційні кампанії після 2014 року, спрямовані на країни Балтії та Україну, продемонстрували, як інформаційні операції можуть посилювати соціальну напругу та впливати на політичні процеси. У порівнянні з попередніми стратегічними концепціями, зокрема 2010 року, де інформаційна безпека згадувалася лише побіжно, документ 2022 року чітко визначає її як стратегічний пріоритет, що вимагає координації між країнами-членами[21].

2. Протидія дезінформації як центральний елемент
Одним із ключових положень Стратегічної концепції 2022 року є акцент на протидії дезінформації як основному інструменту гібридних загроз. Документ визначає дезінформацію як свідоме поширення неправдивої або маніпулятивної інформації для впливу на суспільну думку та політичні рішення. У контексті російсько-українського конфлікту НАТО зазначає, що Росія використовувала

дезінформацію для виправдання своєї агресії, зокрема через наративи про "захист російськомовного населення" чи "нелегітимність" української влади. Для протидії цьому Альянс пропонує багатошаровий підхід, який включає моніторинг інформаційного простору, швидке реагування на фейкові наративи та просування достовірної інформації. Наприклад, Центр стратегічних комунікацій НАТО (StratCom COE) у Ризі відіграє ключову роль у виявленні дезінформаційних кампаній і розробці контрнаративів, що ґрунтуються на фактах. Цей підхід контрастує з холодною війною, коли протидія пропаганді була повільнішою і обмежувалася традиційними медіа, тоді як сучасні стратегії враховують швидкість цифрових платформ[21].

3. Зміцнення когнітивної стійкості

Стратегічна концепція 2022 року вводить концепцію когнітивної стійкості як ключового елемента інформаційної безпеки. Когнітивна стійкість передбачає здатність суспільств і держав протистояти маніпулятивним впливам через підвищення медіаграмотності, критичного мислення та довіри до демократичних інститутів. Документ підкреслює, що країни-члени повинні інвестувати в освітні програми, які навчають громадян розпізнавати дезінформацію та протидіяти психологічним операціям. Наприклад, у Балтійських країнах НАТО підтримує ініціативи з медіаграмотності, які допомагають населенню аналізувати джерела інформації та уникати маніпуляцій[21]. Цей підхід можна порівняти з холодною війною, коли "Радіо Вільна Європа" використовувалося для поширення альтернативних наративів, але сучасні програми є більш інтерактивними та орієнтованими на цифрові платформи, такі як соціальні мережі.

4. Інтеграція кіберзахисту з інформаційною безпекою

Стратегічна концепція 2022 року наголошує на синергії між кіберзахистом і інформаційною безпекою, визнаючи, що кібератаки часто поєднуються з дезінформаційними кампаніями для посилення їхнього ефекту. Наприклад, кібератаки на українську енергетичну систему в 2015-2016 роках супроводжувалися пропагандистськими кампаніями, які звинувачували уряд у

"некомпетентності". У відповідь НАТО підкреслює необхідність розвитку кіберзахисних спроможностей, які включають захист критичної інфраструктури та моніторинг інформаційного простору. Кооперативний центр кіберзахисту (CCDCOE) у Таллінні відіграє важливу роль у розробці стратегій, які інтегрують кібер- та інформаційні операції. Цей підхід відрізняється від холодної війни, коли кіберпростір ще не існував, але нагадує тодішню координацію між розвідкою та пропагандистськими зусиллями для протидії радянським операціям.

5. Співпраця з приватним сектором і партнерами
Документ наголошує на важливості співпраці з приватним сектором, зокрема технологічними компаніями, для протидії інформаційним загрозам. Соціальні мережі, такі як X чи Meta, є основними каналами поширення дезінформації, що вимагає від НАТО партнерства з цими платформами для виявлення та видалення маніпулятивного контенту. Наприклад, у 2024 році було зафіксовано спроби використання ШІ для створення глибоких фейків, які дискредитували лідерів країн НАТО. У порівнянні з холодною війною, коли співпраця обмежувалася державними медіа, сучасний підхід включає ширший спектр акторів, що відображає складність цифрового інформаційного середовища.

6. Стратегічні комунікації як інструмент наступу
Стратегічна концепція 2022 року підкреслює роль стратегічних комунікацій не лише як оборонного, але й як наступального інструменту. НАТО прагне активно формувати наративи, які протидіють ворожій пропаганді та зміцнюють довіру до Альянсу. Наприклад, у відповідь на російські наративи про "агресивність НАТО" Альянс використовує соціальні мережі для поширення інформації про свою миротворчу роль і підтримку партнерів, таких як Україна. Цей підхід має паралелі з холодною війною, коли НАТО використовувало радіо для просування демократичних цінностей, але сучасні стратегії є більш динамічними та таргетованими завдяки цифровим технологіям.

Стратегічна концепція 2022 року закладає основу для комплексного підходу до інформаційної безпеки, який враховує швидкість, масштаби та

складність сучасних гібридних загроз. Вона відображає еволюцію від реактивних заходів холодної війни до проактивних стратегій, які поєднують технологічні, психологічні та соціокультурні інструменти для захисту суспільної свідомості[21].

Брюссельська декларація 2018 року, ухвалена на саміті НАТО в Брюсселі, є одним із ключових документів, що формують доктринальну основу Альянсу для протидії гібридним загрозам, зокрема в контексті інформаційної безпеки. Цей документ відображає реакцію НАТО на зростаючу складність сучасних конфліктів, де гібридні загрози поєднують військові, кібернетичні, інформаційні та економічні методи для дестабілізації країн-членів і партнерів. У порівнянні з періодом холодної війни, коли інформаційна війна обмежувалася протидією пропаганді через традиційні медіа, Брюссельська декларація вводить нові концепції, які враховують швидкість і масштаби цифрового інформаційного простору[22].

Вона підкреслює необхідність комплексного підходу до безпеки, де інформаційна війна розглядається як невід’ємна частина стратегії колективної оборони. Разом із іншими документами, такими як Варшавське комуніке 2016 року та матеріали Центру досконалості з гібридних загроз у Гельсінкі, Брюссельська декларація формує багатошарову доктринальну базу, яка дозволяє НАТО адаптуватися до сучасних викликів, таких як дезінформація, психологічні операції та кібератаки, що використовуються в гібридних конфліктах.

Брюссельська декларація 2018 року є важливим етапом у розвитку стратегій НАТО з протидії гібридним загрозам, оскільки вона вперше чітко артикулює інформаційну безпеку як ключовий елемент колективної оборони. Документ визначає гібридні загрози як комбінацію традиційних і неконвенційних методів, що включають дезінформацію, кібератаки, економічний тиск і використання нерегулярних сил, спрямованих на підрив стабільності країн-членів [22]. У порівнянні з холодною війною, коли НАТО протидіяло радянській пропаганді через радіомовлення, таке як "Радіо Вільна

Європа", Брюссельська декларація акцентує на цифрових викликах, зокрема на ролі соціальних мереж у поширенні маніпулятивного контенту. Наприклад, у контексті російської агресії проти України після 2014 року Росія використовувала платформи, такі як VKontakte і Telegram, для поширення наративів про "громадянську війну" чи "нелегітимність" української влади, що вимагало від НАТО швидшого реагування, ніж у період холодної війни, коли інформація поширювалася повільніше через обмеженість каналів[8].

Одним із центральних положень Брюссельської декларації є визнання гібридних дій як потенційної підстави для активації статті 5 Вашингтонського договору, що розглядає напад на одну країну-члена як напад на всіх. Це положення є значним кроком вперед у порівнянні з попередніми доктринами, такими як Стратегічна концепція 2010 року, де гібридні загрози згадувалися лише побіжно. Декларація наголошує на необхідності посилення стійкості країн-членів до дезінформації через розвиток стратегічних комунікацій і співпрацю з Європейським Союзом[22].

Наприклад, НАТО і ЄС створили спільні центри для аналізу гібридних загроз, такі як Європейський центр досконалості з протидії гібридним загрозам у Гельсінкі, який фокусується на виявленні дезінформаційних кампаній і розробці контрзаходів. Цей підхід має паралелі з холодною війною, коли НАТО координувало інформаційні зусилля з національними урядами для протидії радянській пропаганді, але сучасний контекст вимагає співпраці з приватними технологічними компаніями, такими як Meta чи X, для боротьби з цифровими маніпуляціями[23].

Брюссельська декларація також підкреслює важливість швидкого реагування на гібридні загрози через створення спеціалізованих груп підтримки, які допомагають країнам-членам у разі гібридних атак. Ці групи надають експертизу в таких сферах, як кіберзахист, стратегічні комунікації та аналіз дезінформації, що дозволяє швидко нейтралізувати загрози. У порівнянні з холодною війною, коли подібні зусилля обмежувалися радіомовленням і пресою, сучасні групи підтримки використовують цифрові інструменти для

моніторингу соціальних мереж і аналізу великих даних, що дозволяє виявляти маніпулятивний контент у реальному часі.

Варшавське комуніке 2016 року є ще одним ключовим документом, що формує доктринальну основу НАТО для протидії гібридним загрозам. Ухвалене на тлі російської анексії Криму та війни на Донбасі, це комуніке визначає гібридні загрози як комбінацію військових і невійськових методів, включаючи дезінформацію, кібератаки та економічний тиск, які використовуються для досягнення стратегічних цілей без відкритої війни [24]. У порівнянні з Брюссельською декларацією, Варшавське комуніке більше зосереджується на практичних механізмах, таких як створення гібридних груп підтримки та посилення співпраці з ЄС. Документ підкреслює необхідність інтеграції інформаційної безпеки з кіберзахистом, визнаючи, що гібридні атаки часто поєднують ці елементи для максимального ефекту[24]. Наприклад, кібератаки на українську енергетичну систему в 2015-2016 роках супроводжувалися дезінформаційними кампаніями, які звинувачували уряд у "некомпетентності", що підкреслює синергію між цими методами.

Варшавське комуніке також вводить концепцію стійкості (resilience) як ключового елемента протидії гібридним загрозам. Стійкість передбачає здатність країн-членів протистояти маніпулятивним впливам через зміцнення інфраструктури, підвищення медіаграмотності та розвиток стратегічних комунікацій. У цьому контексті документ закликає до проведення регулярних навчань, таких як Cyber Coalition, які симулюють гібридні атаки, що поєднують кібер та інформаційні елементи. Ці навчання мають паралелі з холодною війною, коли НАТО проводило симуляції для підготовки до радянських пропагандистських кампаній, але сучасні вправи є складнішими через використання цифрових технологій і залучення приватного сектора [24].

Матеріали Європейського центру досконалості з протидії гібридним загрозам у Гельсінкі, створеного в 2017 році, доповнюють Брюссельську декларацію та Варшавське комуніке, надаючи детальний аналіз інформаційних аспектів гібридної війни. Ці документи підкреслюють роль дезінформації як

інструменту для підриву суспільної згуртованості та пропонують моделі для її виявлення, включаючи аналіз соціальних мереж і співпрацю з технологічними компаніями. Наприклад, центр розробив методології для ідентифікації ботів і фейкових акаунтів, які використовуються для ампліфікації маніпулятивного контенту, що було актуальним у контексті російських кампаній проти України[23]. У порівнянні з холодною війною, коли дезінформація поширювалася через фізичні носії, такі як листівки чи газети, сучасні методи вимагають швидшого реагування через цифрові платформи, що робить ці матеріали важливим доповненням до доктринальної бази НАТО.

Центр також акцентує на ролі медіаграмотності як інструменту когнітивної стійкості, що дозволяє населенню розпізнавати маніпулятивний контент. Ці програми нагадують ініціативи холодної війни, такі як "Радіо Свобода", які просували демократичні цінності, але сучасний підхід є більш інтерактивним, використовуючи онлайн-курси та гейміфіковані платформи для залучення молоді.[23].

Ці зусилля демонструють, як НАТО адаптує доктрини до цифрової епохи, зберігаючи уроки холодної війни про важливість суспільної свідомості.

Спільна декларація НАТО-ЄС 2018 року є ще одним важливим документом, що доповнює Брюссельську декларацію, акцентуючи на співпраці між двома організаціями для протидії гібридним загрозам. Документ підкреслює необхідність обміну розвідданими про дезінформаційні кампанії та координації стратегічних комунікацій. Наприклад, у відповідь на російські наративи про "біолабораторії" в Україні, НАТО та ЄС спільно розробляли спростування, які поширювалися через офіційні канали та соціальні мережі [25]. Цей підхід має паралелі з холодною війною, коли НАТО координувало інформаційні зусилля з національними урядами для протидії радянській пропаганді, але сучасна співпраця включає ширший спектр акторів, таких як технологічні компанії, що відображає складність цифрового інформаційного середовища.

Брюссельська декларація та Варшавське комуніке, навпаки, враховують швидкість і масштаби цифрових загроз, де дезінформація може поширюватися за лічені години. Сучасні доктрини НАТО також включають технологічні рішення, такі як аналіз великих даних, що контрастує з холодною війною, коли аналіз інформації був обмежений розвідувальними зусиллями. Крім того, якщо в холодну війну НАТО діяло в умовах чіткого ідеологічного поділу, сучасні гібридні загрози створюють "сіру зону", де межі між війною і миром розмиті, що вимагає від Альянсу більш гнучких доктрин[21].

Брюссельська декларація та Варшавське комуніке пропонують конкретні механізми для реалізації доктрин, включаючи створення спеціалізованих груп підтримки, які допомагають країнам-членам у разі гібридних атак. Ці групи надають експертизу в кіберзахисті, стратегічних комунікаціях і аналізі дезінформації, що дозволяє швидко реагувати на загрози. Наприклад, у 2018 році НАТО надало підтримку Україні для протидії російським дезінформаційним кампаніям, що звинувачували Київ у "геноциді" на Донбасі, використовуючи аналіз соціальних мереж для виявлення фейків[13]. Центр досконалості в Гельсінкі також розробив методології для моніторингу інформаційного простору, що включають використання штучного інтелекту для виявлення ботів і фейкових акаунтів, що є значним прогресом у порівнянні з холодною війною, коли подібні операції були обмежені ручним аналізом.

Іншим важливим механізмом є спільні навчання, які симулюють гібридні атаки. Наприклад, навчання Cyber Coalition включають сценарії, де кібератаки поєднуються з дезінформаційними кампаніями, що дозволяє країнам-членам тестувати свою готовність. Ці вправи нагадують симуляції холодної війни, коли НАТО готувалося до радянських пропагандистських атак, але сучасні навчання є більш складними через використання цифрових технологій і залучення приватного сектора.

Брюссельська декларація та Спільна декларація НАТО-ЄС 2018 року підкреслюють важливість співпраці з партнерами, зокрема ЄС, для протидії

гібридним загрозам. Ця співпраця включає обмін розвідданими, спільні навчання та координацію стратегічних комунікацій. Наприклад, у відповідь на російські дезінформаційні кампанії про "біолабораторії" в Україні, НАТО та ЄС спільно розробляли спростування, які поширювалися через офіційні канали та соціальні мережі. Цей підхід контрастує з холодною війною, коли співпраця обмежувалася національними урядами, але має схожість у координації зусиль для створення єдиного інформаційного фронту. Сучасна співпраця також включає приватний сектор, що дозволяє НАТО швидше виявляти та нейтралізувати маніпулятивний контент.

Усі згадані документи підкреслюють роль медіаграмотності як інструменту когнітивної стійкості. Брюссельська декларація закликає до розвитку освітніх програм, які навчають громадян розпізнавати дезінформацію та аналізувати джерела інформації. Наприклад, у Польщі та Литві НАТО підтримує ініціативи, які допомагають населенню протидіяти російським наративам про "утиски меншин", використовуючи інтерактивні формати, такі як онлайн-курси та гейміфіковані платформи.

Документи НАТО, зокрема Варшавське комуніке, підкреслюють синергію між інформаційною та кібербезпекою, визнаючи, що гібридні атаки часто поєднують ці елементи. Наприклад, кібератаки на українську інфраструктуру в 2015-2016 роках супроводжувалися дезінформаційними кампаніями, що посилювали їхній ефект. У порівнянні з холодною війною, коли кіберпростір ще не існував, сучасні доктрини враховують цифрові загрози, що вимагає від НАТО розвитку технологій для аналізу даних і захисту критичної інфраструктури. Центр досконалості в Гельсінкі пропонує моделі для інтеграції цих аспектів, включаючи використання ШІ для виявлення дезінформації.

Брюссельська декларація, Варшавське комуніке та матеріали Центру досконалості формують міцну доктринальну основу для протидії гібридним загрозам, інтегруючи інформаційну безпеку в стратегії НАТО. Ці документи дозволяють Альянсу адаптуватися до складності сучасних конфліктів,

зберігаючи уроки холодної війни про важливість єдності та стратегічних комунікацій.

Висновки до розділу 1

Отже, дослідження у першому розділі показує що, інформаційна безпека в діяльності НАТО є ключовим елементом протидії гібридним загрозам, що поєднують інформаційні, кібернетичні, економічні та соціокультурні методи впливу, спрямовані на дестабілізацію суспільств і держав. Концепція гібридних загроз, яка набула особливого значення після російської агресії проти України в 2014 році, підкреслює необхідність комплексного підходу, де інформаційний простір визнається окремим доменом операцій, нарівні з традиційними військовими.

Доктринальна еволюція Альянсу відображає адаптацію до нових викликів: від протидії радянській пропаганді в період холодної війни через радіомовлення та пресу до сучасних стратегій, що враховують швидкість і масштаби цифрових платформ. Стратегічна концепція 2022 року, Брюссельська декларація 2018 року та Варшавське комуніке 2016 року формують міцну основу для захисту інформаційного простору, акцентуючи на протидії дезінформації, зміцненні когнітивної стійкості та інтеграції кіберзахисту з інформаційними операціями.

Ці документи підкреслюють важливість співпраці з приватним сектором і партнерами, такими як ЄС, для швидкого реагування на маніпулятивні кампанії, що нагадує координацію зусиль холодної війни, але в новому технологічному контексті. Водночас сучасні доктрини НАТО враховують унікальні виклики цифрової епохи, такі як використання штучного інтелекту та соціальних мереж для ампліфікації дезінформації, що вимагає від Альянсу гнучкості та інноваційних рішень для забезпечення безпеки країн-членів і партнерів.

РОЗДІЛ 2. НАТО У ПРОТИДІЇ РОСІЙСЬКІЙ ДЕЗІНФОРМАЦІЇ ТА ЗАХОДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Роль НАТО у протидії російській дезінформації проти України з 2014 року

Після 2014 року інформаційний фронт став одним із ключових елементів гібридної агресії Росії проти України. Анексія Криму та початок війни на Донбасі супроводжувалися масштабними дезінформаційними кампаніями, які Кремль розгортав не лише проти українського суспільства, а й у міжнародному інформаційному просторі. Основним завданням цих кампаній було делегітимізувати українську владу, підірвати довіру до демократичних інститутів, посіяти розкол у суспільстві та виправдати російську військову експансію.

Варто відзначити, що ключові наративи, які активно просувалися з 2014 року, включали ідею так званої «громадянської війни» на сході України, необхідність «захисту російськомовного населення» та твердження про «нелегітимність української влади». Згодом ці меседжі доповнювалися новими, зокрема міфами про нібито існування в Україні «біолабораторій США», які створювали образ країни як загрози не лише для Росії, але й для всього світу [26]. Така стратегія дозволяла Кремлю адаптувати пропаганду під конкретний міжнародний контекст, використовуючи страхи та упередження цільової аудиторії.

У своїй основі ці методи мали очевидні паралелі з радянською пропагандою часів холодної війни. І тоді, і тепер використовувалися емоційно насичені меседжі, які спиралися на дихотомію «свій — чужий», створювали образ «ворога» та апелювали до загроз для безпеки простих громадян. Проте відмінність сучасного етапу полягає у використанні цифрових платформ, які дозволяють поширювати повідомлення практично миттєво, охоплюючи мільйони людей по всьому світу. Така швидкість і масштабність робили дезінформацію набагато небезпечнішою, ніж у XX столітті, коли канали комунікації були значно обмеженішими.

Особливу увагу Кремль приділяв впливу на суспільну думку як усередині України, так і в країнах Центральної Європи — зокрема Польщі та Чехії. У цих державах активно поширювалися тези про «втому від України», «неефективність української влади» чи «загрозу для європейської стабільності через війну». Водночас у глобальному контексті просувалася риторика про «небажання Заходу підтримувати Київ», що мало підірвати міжнародну солідарність на користь України.

Російська дезінформація після 2014 року стала не лише засобом виправдання агресії, але й способом системного впливу на суспільства у регіональному та міжнародному масштабі, що сформувало нову конфігурацію інформаційного протистояння [27].

Інформаційна війна після 2014 року поступово перетворилася на стратегічний інструмент російської зовнішньої політики, який був інтегрований у військові, дипломатичні та економічні операції. Дезінформація стала основою тактики «керованого хаосу», покликаної послаблювати інститути держави та створювати у міжнародної спільноти сумніви щодо правомірності дій України. Саме в цей період з’явилися численні приклади скоординованих медійних атак, коли меседжі з офіційних російських каналів синхронізувалися з активністю бот-мереж і проросійських медіа у країнах ЄС [27].

Важливо підкреслити, що такі кампанії не обмежувалися лише поширенням неправдивої інформації. Вони активно комбінували маніпуляцію фактами з використанням напівправди, а також із викривленням реальних подій. Це дозволяло створювати наративи, які здавалися більш переконливими для іноземної аудиторії. Наприклад, у Польщі та Словаччині Росія просувала тези про нібито «економічну загрозу від українських біженців», що посилювало антиміграційні настрої у цих суспільствах.

Змінилася й мета пропагандистських атак: якщо раніше вони були спрямовані насамперед на підрив довіри до української влади, то після 2014 року вони стали ширшими, орієнтуючись на дискредитацію самої ідеї європейської солідарності. У медіапросторі активно культивувалися наративи

про «розкол Заходу», «неефективність ЄС» та «агресивну політику НАТО», що мало завданням зменшити підтримку України у ключових міжнародних столицях [28].

Анексія Криму та початок війни на Донбасі стали для НАТО сигналом, що інформаційна сфера є не менш важливим полем бою, ніж традиційні військові простори. Уже у 2014 році Альянс визнав дезінформацію складовою гібридної війни, що застосовується Росією проти України та сусідніх держав. Відповіддю стало формування нових стратегій у сфері стратегічних комунікацій, розробка інституційних механізмів боротьби з фейками та координація дій з ЄС і національними урядами. Важливою віхою стало створення у 2015 році Центру стратегічних комунікацій НАТО у Ризі, який спеціалізувався на моніторингу дезінформаційних кампаній та розробці практичних інструментів протидії [29].

Особливу увагу Альянс приділив взаємодії з країнами Центральної та Східної Європи, які виявилися найбільш уразливими до російських інформаційних атак. Було розпочато систематичне навчання державних структур та військових у сфері кіберзахисту і стратегічних комунікацій, що дозволило швидше реагувати на сплески пропаганди. Одним із ключових елементів стала співпраця з Україною, яка надавала унікальний досвід протидії російській дезінформації у реальних умовах війни.

НАТО також активно впроваджувало інформаційні кампанії, спрямовані на пояснення власних дій та демонстрацію прозорості. Це мало зменшити ефективність російських наративів про «агресивний блок НАТО», які активно поширювалися у міжнародному інформаційному просторі. Важливим кроком стало використання соціальних мереж та цифрових платформ самим Альянсом: якщо у попередні десятиліття НАТО спирався переважно на традиційні ЗМІ, то після 2014 року він інтегрував цифрові канали комунікації, щоб безпосередньо доносити інформацію до суспільств країн-членів і партнерів [30].

Ще одним напрямом відповіді стало розширення співпраці з незалежними фактчекінговими організаціями та аналітичними центрами.

НАТО не прагнув монополізувати протидію дезінформації, натомість заохочував створення багаторівневої системи, де державні й недержавні актори працюють разом. Це дозволяло не лише швидко спростовувати неправдиві повідомлення, але й зміцнювати довіру громадськості до процесу перевірки фактів.

Усе це свідчить про те, що після 2014 року Альянс поступово перейшов від ситуативної реакції на російські інформаційні операції до системного підходу, де інформаційна безпека стала одним із ключових напрямів колективної оборони.

Поступове усвідомлення масштабу російських інформаційних кампаній змусило Альянс зміцнити власну аналітичну спроможність. Уже у 2016-2017 роках НАТО активно розгорнуло співпрацю з Європейською службою зовнішніх дій та її підрозділом East StratCom Task Force, що спеціалізувався на викритті російської дезінформації в ЄС. Ця взаємодія дозволяла оперативно обмінюватися даними про нові фейкові наративи, які поширювалися від Балтії до Балкан, та узгоджувати контрзаходи. Для НАТО було принципово важливо не лише відслідковувати пропаганду, але й забезпечувати багаторівневу координацію з демократичними інституціями Європи [31].

Водночас Альянс усвідомив, що ефективність протидії залежить від довіри громадян. Тому після 2018 року стратегічні комунікації НАТО почали зміщувати акцент від суто оборонного реагування на дезінформацію до проактивного формування позитивних історій про власну діяльність. Це передбачало використання зрозумілої мови, візуальних матеріалів та прикладів, які робили діяльність організації ближчою до пересічних громадян. Такий підхід дозволяв поступово нейтралізувати російські наративи про «відрив НАТО від реальних потреб населення» [31].

Особливу увагу приділили цифровим платформам і кіберпростору. Паралельно зі створенням підрозділів, що моніторили соціальні мережі, Альянс інвестував у розвиток технологічних інструментів штучного інтелекту для виявлення бот-мереж і скоординованої неавтентичної активності. Такі

алгоритми дозволяли швидше ідентифікувати інформаційні вкиди, а також прогнозувати їхній можливий вплив на аудиторії. Таким чином, НАТО поступово адаптував власну діяльність до умов цифрової епохи, де швидкість поширення інформації стала ключовим фактором успіху [32].

Іншим важливим напрямом стала робота з партнерами поза межами Європи. Адже російська дезінформація не обмежувалася лише українським чи європейським контекстом, вона активно поширювалася в Африці, Латинській Америці та на Близькому Сході, де наративи Кремля знаходили вдячний ґрунт. НАТО через партнерські програми почав розвивати механізми стратегічних комунікацій для третіх країн, що дозволяло водночас протидіяти російському впливу та зміцнювати власну міжнародну легітимність [32].

Продовжуючи тему, важливо відзначити, що частиною комплексної стратегії НАТО стала підготовка фахівців із протидії дезінформації в країнах-партнерах. Альянс активно розгорнув освітні програми та тренінги для журналістів, аналітиків і державних службовців, зокрема у Центральній та Східній Європі, спрямовані на розвиток навичок розпізнавання фейкових новин, оцінки достовірності джерел і виявлення маніпулятивних наративів. Такі заходи дозволяли не лише зміцнити національні системи інформаційної безпеки, а й створювали ефект «ланцюгової реакції», коли підготовлені фахівці могли поширювати знання серед медіа та громадських організацій.

Одночасно в рамках програм НАТО для держав-членів і партнерів проводилися симуляції та навчальні ігри з моделювання інформаційних атак, що допомагало відпрацювати практичні навички реагування на кризові ситуації. Завдяки таким тренінгам учасники отримували можливість оперативно ідентифікувати спроби маніпуляції, формувати контрзаходи та координувати дії з міжнародними партнерами. Це створювало додатковий рівень захисту від російських дезінформаційних кампаній, підвищуючи стійкість інформаційного середовища в регіоні [33].

Ще одним аспектом була співпраця з медіа та академічними інституціями. НАТО підтримував розробку аналітичних платформ і баз даних

для відстеження та систематизації російських наративів, надаючи доступ до них журналістам, дослідникам і урядовим органам. Це дозволяло створювати більш об'єктивні контрнаративи та поширювати їх через авторитетні канали, одночасно формуючи у громадськості критичне мислення та здатність до самостійної перевірки інформації. Такі ініціативи мали довгостроковий ефект, адже підвищували загальний рівень медіаграмотності та сприяли розвитку інформаційної екосистеми, стійкої до маніпуляцій.

Таким чином, діяльність НАТО у сфері освіти та тренінгів, а також співпраця з медіа і науковими установами, створювала багатошаровий захисний механізм проти російської дезінформації, поєднуючи превентивні, аналітичні та практичні заходи. Цей комплексний підхід демонструє, що боротьба з гібридними загрозами вимагає не лише технічних рішень, але й послідовної роботи з людським фактором — ключовим елементом сучасної інформаційної безпеки.

Розглядаючи оперативні дії НАТО у сфері протидії російській дезінформації після 2014 року, варто зазначити, що Альянс зосередився на трьох ключових напрямках: стратегічному моніторингу, оперативному реагуванні та міжнародній координації.

Перший із них включав систематичне відстеження медіапростору та соціальних платформ на предмет поширення антиукраїнських наративів, що дозволяло ідентифікувати нові методи маніпуляцій та прогнозувати їхню потенційну шкоду для суспільної думки. Застосування аналітичних інструментів, включно з платформами для автоматизованого збору та класифікації контенту, стало критично важливим для швидкого реагування на масові дезінформаційні кампанії [34].

Другий напрямок передбачав безпосереднє протидіяння через публічні заяви, інформаційні кампанії та координацію з урядами партнерських держав. НАТО активно поширював перевірені дані та аналітичні звіти щодо дій Росії, водночас сприяючи формуванню контрнаративів, які знижували вплив маніпуляцій. Наприклад, у період ескалації на Донбасі 2014-2015 років Альянс

підтримував українські урядові комунікаційні платформи та інформаційні центри в країнах Центральної Європи, спрямовані на інформування громадськості про реальний стан справ на фронті та розвінчання міфів щодо «громадянської війни» [34].

Третій аспект — міжнародна координація. НАТО активно взаємодіє з ЄС, ОБСЄ, державами-членами та іншими міжнародними організаціями для обміну інформацією про російські дезінформаційні кампанії. Така співпраця дозволяє швидко реагувати на нові загрози, уніфікувати методики протидії та розробляти спільні навчальні програми для підвищення медіаграмотності на рівні держав. Одним із практичних результатів цієї координації стала стандартизація методів відстеження та оцінки впливу дезінформації, що сприяло більш ефективній роботі національних центрів стратегічних комунікацій [34].

У комплексі ці заходи показують, що протидія російській дезінформації вимагає інтегрованого підходу, поєднання технологічних рішень, аналітичної роботи та міжнародної координації, що дозволяє реагувати не лише на існуючі загрози, а й прогнозувати їхню еволюцію у майбутньому.

Російські інформаційні кампанії після 2014 року значно вплинули на формування громадської думки як в Україні, так і в сусідніх країнах Центральної Європи, а також на глобальному рівні. Внутрішньоукраїнський контекст характеризувався поширенням наративів про «нелегітимність влади», «громадянську війну» та «захист російськомовного населення», які викликали розкол у сприйнятті подій серед населення, посилюючи суспільну тривожність та недовіру до державних інституцій. Ці наративи активно поширювалися через соціальні мережі, месенджери та нові цифрові платформи, створюючи інтенсивне інформаційне середовище, в якому реальні факти часто губилися серед маніпулятивних повідомлень [35].

У країнах Центральної Європи, зокрема Польщі та Чехії, російські кампанії намагалися формувати скептичне ставлення до підтримки України, апелюючи до історичних та культурних стереотипів. Використання цифрових

каналів дозволяло таргетувати окремі соціальні групи, створюючи ілюзію ширшої підтримки проросійських поглядів. Аналітики відзначають, що такі наративи здатні посилювати політичну поляризацію та підривати довіру до європейських інституцій, що потенційно впливає на прийняття рішень щодо допомоги Україні [35].

На глобальному рівні дезінформаційні кампанії прагнули формувати негативний образ України як нестабільної та корумпованої держави, одночасно зменшуючи легітимність міжнародної підтримки Києва. Застосування масових бот-мереж, coordinated trolling та автоматизованих систем поширення повідомлень забезпечувало значне охоплення та вплив на міжнародну аудиторію, зокрема через соціальні медіа, платформи відеоконтенту та англомовні інформаційні ресурси.

Такі кампанії продемонстрували здатність гібридних інформаційних стратегій поєднувати класичні методи пропаганди з новими технологічними інструментами, що дозволяє Росії оперативно адаптувати наративи під змінні обставини та впливати на міжнародний дискурс. Водночас реакція суспільства та урядових структур показала, що боротьба з дезінформацією потребує комплексного підходу, який включає підвищення медіаграмотності, аналітичну роботу та міжнародну координацію дій.

2.2. Заходи НАТО з інформаційної безпеки в умовах кібератак

З ростом складності та інтенсивності кіберзагроз НАТО підкреслює необхідність тісної інтеграції кіберзахисту та інформаційної безпеки. Під час Брюссельського саміту 2021 року Альянс затвердив Комплексну політику кібероборони, що передбачає не лише захист власної інфраструктури, але й активний моніторинг та протидію інформаційним загрозам, які супроводжують кібератаки. Особливу увагу приділено гібридним сценаріям, коли цифрові атаки поєднуються з дезінформаційними кампаніями для впливу на громадську думку та міжнародну позицію [36].

Приклади останніх років демонструють, наскільки інтегрований підхід є ефективним. Так, у 2022-2023 роках НАТО реагувало на скоординовані кібератаки проти критичної інфраструктури України, які супроводжувалися масовим поширенням фейкових новин про нібито провал оборони та нестачу ресурсів. Альянс підтримував українські органи кібербезпеки через обмін розвідданими, технічну допомогу та навчальні програми, що дозволяло зменшити вплив одночасних кібер- та інформаційних атак.[37].

Ще одним прикладом є 2023 рік, коли атаки з використанням шкідливого програмного забезпечення типу WhisperGate поєднувалися з кампаніями в соцмережах, спрямованими на дискредитацію урядових структур. У відповідь НАТО активно застосовувало систему моніторингу кіберактивності та аналізу дезінформаційних потоків, що дозволяло своєчасно виявляти та блокувати ключові загрози [38].

Інтеграція кібер- та інформаційної безпеки дозволяє Альянсу не лише реагувати на атаки, але й прогнозувати потенційні вектори впливу противника. Висока адаптивність російських гібридних кампаній змушує НАТО постійно оновлювати стандарти кіберзахисту, включаючи аналіз поведінки користувачів, відстеження бот-мереж та виявлення координованих маніпуляцій у медіапросторі. Такий підхід підкреслює необхідність постійного поєднання технічних, стратегічних та інформаційних заходів для забезпечення цілісної оборони союзників і партнерів.

Розвиток кіберінфраструктури НАТО та інтегрованих систем моніторингу інформаційних загроз став ключовим елементом протидії сучасним гібридним атакам. У 2024 році Альянс акцентував увагу на створенні Центру передового досвіду з кібероборони та інформаційної безпеки, який об’єднує аналітичні ресурси, технології штучного інтелекту та експертні знання для своєчасного виявлення дезінформаційних кампаній. Це дозволяє не лише реагувати на поточні загрози, а й прогнозувати потенційні вектори атаки, включаючи координацію кібератак та онлайн-пропаганди [39].

Особливої уваги потребує швидкість реагування на багатовекторні загрози. Наприклад, у 2023-2024 роках фіксувалися кампанії, коли дезінформаційні повідомлення про нестачу гуманітарної допомоги та нібито зради з боку українських лідерів поширювалися синхронно з кібератаками на державні портали. Завдяки інтегрованим протоколам обміну розвідданими та застосуванню систем раннього попередження НАТО змогло локалізувати ключові інформаційні осередки та мінімізувати ефект маніпуляцій [38].

Застосування аналітики великих даних і алгоритмів машинного навчання дозволяє Альянсу оцінювати ефективність інформаційних атак, визначати цільові аудиторії та прогнозувати ймовірні теми майбутніх кампаній. У 2025 році було запроваджено нові модулі для аналізу поведінки користувачів у соцмережах, що дозволяють відокремлювати організовані бот-мережі від реальної активності населення, а також визначати джерела координації дезінформації [39].

Одним із стратегічних напрямів є також посилення співпраці НАТО з державами-партнерами у сфері кібербезпеки та медіаграмотності. Спільні навчання, симуляції кібератак та обмін досвідом щодо протидії дезінформації підвищують готовність союзників швидко реагувати на гібридні загрози та підтримувати стійкість інформаційного середовища.

У результаті інтеграція кібер- та інформаційної безпеки стає не лише технічним завданням, а й складовою стратегічного управління сучасними загрозами. Її ефективність залежить від постійного оновлення методів аналізу, швидкості реагування на багатовекторні кампанії та тісної взаємодії між союзниками, що створює комплексний механізм протидії російській дезінформації та кібератакам на Україну та країни-союзники.

Після початку повномасштабного вторгнення Росії у 2022 році НАТО значно посилило підтримку України у сфері кібер- та інформаційної безпеки, приділяючи увагу комплексній інтеграції технічної допомоги, навчальних програм та обміну досвідом. Одним із ключових інструментів стала співпраця через Кооперативний центр кіберзахисту (CCDCOE) у Таллінні, який надає

консультації щодо захисту критичної інфраструктури, проводить спеціалізовані навчання для державних органів та критично важливих підприємств, а також розробляє методики оцінки ймовірних загроз від гібридних атак [40].

У 2023-2024 роках НАТО фокусувався на забезпеченні оперативного реагування на сучасні кібератаки, які супроводжуються активними дезінформаційними кампаніями. Наприклад, українські державні портали та платформи, що інформують населення, ставали мішенями координаційних атак, де цифрові вторгнення поєднувалися з масовим поширенням фейкових новин про перебіг бойових дій або нібито «зраду» української влади. В рамках співпраці НАТО надавав технічну підтримку для локалізації джерел атак, відновлення функціонування систем та нейтралізації ефекту дезінформаційного впливу [40].

Крім технічних аспектів, увага приділялася підвищенню кібергігієни та медіаграмотності серед українських службовців і населення. Спільні навчання з українськими силами безпеки дозволяють відпрацьовувати сценарії комплексних гібридних атак, де кібер- та інформаційні операції поєднуються для створення хаосу та дестабілізації. Такі практики сприяють не лише покращенню здатності до швидкого реагування, а й формують базу для розробки контрнаративів, здатних зменшити вплив російських інформаційних кампаній [41].

Важливим напрямом є також посилення взаємодії між різними гілками української влади та союзниками НАТО, що дозволяє більш оперативно обмінюватися даними про потенційні загрози, оцінювати їхню масштабність та координувати контрзаходи. Ця синергія технічної допомоги, навчання та стратегічного планування створює системний підхід до протидії гібридним загрозам і дозволяє Україні поступово підвищувати рівень стійкості національної інформаційної та кібербезпеки [41].

Паралельно з технічною підтримкою НАТО активно впроваджуються програми стратегічного моніторингу та раннього попередження щодо кібератак і дезінформаційних кампаній. Зокрема, Україна отримує допомогу в побудові

систем, здатних відстежувати потенційні загрози в реальному часі, аналізувати поведінку мережевих ботів, виявляти фейкові акаунти та координовані атаки на інформаційні ресурси. Такий підхід дозволяє не лише зменшити шкоду від конкретних кіберінцидентів, а й прогнозувати ймовірні напрями майбутніх атак, що є критично важливим для забезпечення безперервності державних служб та комунікаційних каналів.

Крім технічних інструментів, НАТО активно підтримує розвиток людського потенціалу в Україні. Це включає навчальні програми для аналітиків, фахівців з кібербезпеки та журналістів, які займаються перевіркою фактів і протидією дезінформації. Ці заходи спрямовані на створення цілісної системи інформаційного захисту, де кожен компонент - від державних органів до медіа - володіє знаннями та навичками для протидії гібридним загрозам [42].

Особливої уваги заслуговує координація дій НАТО з українськими структурами у сфері кібер-розвідки та аналізу загроз. Спільні ініціативи дозволяють інтегрувати дані з різних джерел, оцінювати потенційний вплив атак на критичну інфраструктуру та оперативно розробляти алгоритми реагування. Така інтеграція значно підвищує ефективність заходів безпеки, одночасно мінімізуючи ризик масштабного поширення дезінформації та паніки серед населення.

Ключовим аспектом сучасної допомоги НАТО є також розвиток інструментів прогнозування та моделювання інформаційних атак. За допомогою аналітичних платформ та симуляційних моделей можна оцінювати потенційні сценарії розвитку дезінформаційних кампаній, визначати критичні вузли у інформаційному просторі та розробляти стратегії попередження кризових ситуацій. Такий підхід створює передумови для більш стійкого інформаційного середовища та дозволяє Україні швидко адаптуватися до змінних умов гібридної війни.

Після 2016 року країни Центральної Європи, зокрема Польща, стали важливими майданчиками для впровадження заходів НАТО у сфері кібер- та інформаційної безпеки. Російські операції проти цих держав демонструють

високий рівень координації між кіберактивністю та дезінформаційними кампаніями. Наприклад, у січні 2025 року польська влада повідомила про виявлення російської групи, яка, за її даними, мала на меті вплинути на польські вибори шляхом поширення дезінформації та дестабілізації політичної ситуації. Ці дії, за словами польського віцепрем'єр-міністра Кшиштофа Гавковського, були спрямовані на підрив довіри до демократичних інститутів та посилення політичної поляризації в країні[43].

Аналогічні кампанії у Чехії також були спрямовані на дискредитацію виборчих процесів і посилення політичної поляризації, використовуючи локальні медіа й соціальні мережі для максимального охоплення аудиторії.

Ці приклади підтверджують необхідність посилення співпраці між країнами Центральної Європи та НАТО у сфері кібербезпеки та інформаційної стійкості.

Ключовим інструментом практичної підготовки стала навчальна ініціатива Cyber Coalition, що включає симуляції гібридних атак з одночасним поєднанням кіберактивності та дезінформаційних кампаній. Учасники мають змогу тестувати координацію між національними структурами, обмінюватися досвідом і перевіряти готовність до реагування на багатовимірні загрози. Такий підхід сприяє підвищенню колективної стійкості Центральної Європи до інформаційно-кіберних атак, створюючи умови для формування інтегрованої стратегії безпеки, здатної протидіяти сучасним викликам гібридної війни[44].

Сучасний досвід Центральної Європи демонструє, що успішна протидія гібридним загрозам потребує комплексного підходу, який поєднує технічні, організаційні та інформаційні складові. Окрім розбудови кіберінфраструктури та оперативного реагування на кібератаки, країни регіону активно впроваджують механізми боротьби з дезінформацією, що включають медіаосвіту населення, моніторинг соціальних мереж та створення швидких каналів для спростування фейкових новин. Такі заходи дозволяють не лише знижувати ефект масової паніки, спричиненої інформаційними кампаніями

противника, а й формувати стійкіший інформаційний простір, який важко піддати маніпуляціям.

НАТО, у рамках своєї стратегічної концепції, приділяє особливу увагу інтеграції національних систем захисту з альянсовими платформами, що забезпечує спільне відстеження загроз і швидкий обмін розвідданими. Наприклад, багатосторонні навчання та симуляції гібридних атак дозволяють відпрацьовувати координацію між урядовими органами, оборонними структурами та незалежними медіа, створюючи своєрідний "живий щит" проти поширення дезінформації.

Водночас досвід Польщі та Чехії підкреслює важливість адаптації стратегій НАТО до локальних умов та культурного контексту. У країнах Центральної Європи значна частина населення піддається впливу російських наративів через історично сформовані стереотипи та медіаекспозицію. Саме тому поєднання кіберзахисту з інформаційною роботою та освітою громадян стає ключовим елементом стійкості. Такий підхід дозволяє не лише нейтралізувати конкретні атаки, а й знижувати ймовірність успішного впливу на громадську думку у довгостроковій перспективі.

Крім того, Центральна Європа демонструє зростаючу роль аналітики та прогнозування. Використання даних про кіберінциденти, соціальні тренди та активність у мережах дозволяє оцінювати потенційні ризики завчасно та коригувати політики реагування. Це особливо важливо у контексті швидкоплинних дезінформаційних кампаній, де затримка у виявленні або реакції може призвести до масштабних наслідків як у медійному просторі, так і на політичному рівні. Таким чином, формування адаптивної, інтегрованої системи захисту стає визначальним чинником ефективності НАТО у Центральній Європі.

Сучасна оцінка заходів НАТО щодо протидії гібридним загрозам у Центральній Європі демонструє певний прогрес у сфері кіберзахисту та інформаційної стійкості. Впроваджені механізми, включаючи багатосторонні навчання, інтеграцію національних систем моніторингу з платформами альянсу

та розробку швидких протоколів реагування, дозволили значно зменшити вплив окремих кібератак на критичну інфраструктуру держав-членів. У Польщі та Чехії відзначено покращення координації між урядовими структурами, оборонними агентствами та незалежними організаціями, що стало можливим завдяки активній участі CCDCOE у розробці методик виявлення та нейтралізації гібридних загроз[45][46].

Проте швидкість розвитку кібератак і складність синхронізації дій у реальному часі залишаються серйозним викликом. Нові цифрові технології дозволяють противнику запускати багатовекторні операції, поєднуючи дезінформаційні кампанії з кібератаками на енергетичну та комунікаційну інфраструктуру. Такі комбінації створюють ефект подвійного тиску, коли одночасно завдаються технічні та психологічні удари, що ускладнює оцінку ефективності окремих заходів реагування.

З погляду інформаційної стабільності, дезінформаційні кампанії продовжують впливати на громадську думку, особливо у регіонах із високим рівнем сприйнятливості до антизахідних наративів. Незважаючи на наявність офіційних каналів спростування та кампаній з медіаосвіти, частина населення все ще піддається маніпуляціям, що підкреслює необхідність комплексного підходу до інформаційної безпеки, який включає не лише технічні, а й освітні, аналітичні та комунікаційні компоненти.

Оцінка ефективності показує, що НАТО здатне значно зменшити ризики гібридних атак завдяки координації та технологічним інструментам, однак постійне оновлення методик, адаптація до нових цифрових загроз та збільшення інвестицій у навчання персоналу і модернізацію інфраструктури залишаються критично важливими для підтримки високого рівня готовності. Такий підхід дозволяє державам-членам альянсу не лише реагувати на наявні загрози, а й прогнозувати потенційні сценарії розвитку дезінформаційних та кіберактивностей противника, формуючи більш стійкий інформаційний простір [47].

Розвиток гібридних загроз у Центральній Європі демонструє, що традиційні моделі реагування на кібератаки та дезінформацію вже не забезпечують достатнього рівня захисту. Складність сучасних операцій полягає не лише у технічних аспектах, а й у психологічному ефекті, який створює швидке та масове поширення фейкових повідомлень через соціальні мережі та месенджери.

Це змушує НАТО та національні уряди переглядати підходи до інформаційної безпеки, інтегруючи превентивні заходи з аналітикою поведінки користувачів, алгоритмами виявлення аномалій та симуляціями потенційних атак. Важливим компонентом стає здатність прогнозувати, які наративи будуть найбільш ефективними для впливу на різні групи населення, і відповідно планувати комунікаційні стратегії для їх нейтралізації.

Також значну увагу приділяють об’єднанню міжнародних зусиль, що дозволяє швидше обмінюватися даними про активність кібератак і дезінформаційних кампаній. Платформи координації, які поєднують аналітичні ресурси НАТО та національних центрів кібербезпеки, забезпечують виявлення загроз у режимі реального часу та формують рекомендації щодо оперативних контрзаходів. Такий підхід не лише знижує ризик технічного проникнення, а й допомагає формувати стійкість громадської думки до маніпуляцій [47].

Водночас, динамічність сучасних гібридних операцій потребує постійного оновлення навичок персоналу, розширення інструментарію цифрової безпеки та інвестицій у навчальні програми для підвищення медіаграмотності населення. Це створює передумови для більш комплексного захисту інформаційного простору, де поєднуються технічні, психологічні та стратегічні аспекти, здатні протидіяти сучасним загрозам, які постійно трансформуються та ускладнюються.

Розширення співпраці НАТО з приватним сектором відображає сучасні тенденції у розвитку інформаційної та кібербезпеки, де швидкість обробки великих обсягів даних і здатність виявляти аномалії в режимі реального часу стають критично важливими. Приватні компанії, що спеціалізуються на

аналітиці даних, кіберзахисті та штучному інтелекті, надають Альянсу технологічні ресурси, які дозволяють відслідковувати підозрілу активність у цифровому просторі та оцінювати потенційні загрози до їх реалізації. Використання таких інструментів у поєднанні з військовими та урядовими ресурсами створює комплексну систему превентивного реагування, здатну своєчасно виявляти та нейтралізувати інформаційні та кібератаки.

Координація з Європейським Союзом розширює горизонт партнерства, забезпечуючи обмін розвідданими та спільну розробку стратегій захисту критичної інфраструктури. Спільні центри кібербезпеки та інтегровані платформи обміну інформацією дозволяють швидко оцінювати потенційні ризики та виробляти узгоджені відповіді на загрози, що комбінують технічні та психологічні методи впливу. Це сприяє формуванню більш стабільного інформаційного середовища, де реакція на дезінформаційні кампанії та кібератаки відбувається координаційно та системно [48].

Інновації у сфері моніторингу інформаційного простору включають застосування алгоритмів штучного інтелекту для аналізу потоків даних, виявлення аномалій та прогнозування потенційного впливу дезінформаційних кампаній на громадську думку. Використання таких технологій дозволяє не лише швидко реагувати на кібератаки, а й розробляти стратегічні сценарії протидії, моделювати наслідки інформаційних кампаній та планувати превентивні комунікаційні заходи. Це особливо актуально у контексті російських гібридних операцій, які поєднують цифрові атаки, медіаманіпуляції та психологічний тиск, створюючи багатовимірний вплив на суспільство [48].

Крім технологічних та аналітичних аспектів, важливим елементом інноваційних заходів НАТО є впровадження платформ для обміну інформацією в режимі реального часу, що дозволяє країнам-членам швидко реагувати на загрози та координувати дії у випадку гібридних атак. Такі платформи забезпечують інтеграцію даних з різних джерел — від державних органів до приватного сектору та міжнародних партнерів — що дозволяє формувати комплексне уявлення про поточні загрози та потенційні сценарії розвитку

подій. Це особливо актуально у випадку комбінованих дій противника, коли кібератаки супроводжуються активним розповсюдженням дезінформації, створюючи тиск на суспільну думку та дезорганізуючи державні структури.

Додатково Альянс активно розвиває навчальні програми та симуляційні тренування для персоналу держав-членів і партнерів, зокрема щодо реагування на гібридні та кібератаки. Це включає моделювання сценаріїв, у яких кібератаки поєднуються з маніпуляціями у медіапросторі, дозволяючи учасникам оцінити ефективність превентивних заходів, відпрацювати алгоритми координації та вдосконалити протоколи швидкого реагування. Такі навчання сприяють формуванню колективного досвіду у боротьбі з комплексними загрозами та підвищують готовність до кризових ситуацій, що мають одночасно інформаційний та технологічний характер.

Підвищення ефективності інформаційної безпеки НАТО в умовах сучасних гібридних загроз неможливе без тісної співпраці між державними структурами, міжнародними організаціями та приватним сектором. Одним із ключових аспектів такої взаємодії є розвиток технологій аналізу великих даних та виявлення кіберзагроз у реальному часі, що дозволяє прогнозувати потенційні атаки та оперативно реагувати на них. Співпраця з технологічними компаніями сприяє створенню інноваційних інструментів, здатних відстежувати масові дезінформаційні кампанії, ідентифікувати автоматизовані бот-мережі та виявляти координовані атаки на інформаційний простір.

НАТО активно координує свої дії з Європейським Союзом, обмінюючись розвідданими та розробляючи спільні стандарти кіберзахисту. Спільні центри та платформи дозволяють інтегрувати інформаційні та кіберзахисні заходи, формуючи єдиний механізм реагування на гібридні загрози. Додатково, міжурядові організації, такі як ООН та ОБСЄ, надають експертну підтримку, проводять аудит систем безпеки та розробляють методології протидії дезінформаційним кампаніям, що забезпечує більш ефективну координацію між державами-членами НАТО та країнами-партнерамих[48]

Велику роль відіграє залучення громадянського суспільства та відкритих платформ для моніторингу інформаційного простору. Інструменти, що дозволяють журналістам, аналітикам та організаціям незалежно відстежувати поширення фейкових наративів, значно розширюють механізми реагування на загрози та підвищують цифрову стійкість суспільства.

Водночас розвиток новітніх технологій, зокрема генеративного штучного інтелекту, deepfake та автоматизованих бот-мереж, ставить перед НАТО виклики швидкої адаптації стратегій та інструментів. Підвищення складності атак і їхня висока швидкість вимагають постійного оновлення аналітичних платформ, навчання персоналу та мобілізації ресурсів на міжнародному рівні, що є критично важливим для ефективного захисту критичної інфраструктури та інформаційного простору союзників.

2.3. Сучасні виклики інформаційної безпеки та роль НАТО у їх подоланні

Сучасний світ стикається з безпрецедентними викликами в галузі інформаційної безпеки, які вимагають комплексного підходу для їх вирішення. З розвитком технологій та зростанням кількості кібератак, дезінформації та інших форм інформаційних загроз, забезпечення інформаційної безпеки стало одним з ключових пріоритетів для міжнародних організацій, зокрема НАТО. Ці виклики особливо актуальні в контексті сучасних конфліктів, де інформація та дезінформація відіграють важливу роль. Розвиток штучного інтелекту, технологій дипфейків та кібербезпеки створює нові можливості для захисту інформації, але також і нові ризики, які необхідно враховувати при розробці стратегій інформаційної безпеки.

Технологія дипфейків, яка дозволяє створювати реалістичні відео та аудіо записи з використанням штучного інтелекту, стала одним з найсерйозніших викликів для інформаційної безпеки. Дипфейки можуть бути використані для маніпуляції громадською думкою, поширення дезінформації та

дестабілізації суспільства. Наприклад, у 2024 році було зафіксовано кілька випадків використання дипфейків для поширення дезінформації щодо конфлікту в Україні. Ці відео були розроблені для того, щоб викликати паніку та недовіру серед населення. НАТО активно працює над розробкою методів виявлення та протидії дипфейкам, включаючи використання передових технологій штучного інтелекту для аналізу та виявлення фальшивих відео та аудіо записів. Одним з прикладів успішного використання дипфейків є випадок, коли фальшиве відео з президентом України було поширене в соціальних мережах з метою дестабілізації ситуації в країні. Це відео було швидко виявлено та спростовано завдяки співпраці між НАТО та українськими спецслужбами[49].

Цей випадок підкреслює важливість міжнародної співпраці та використання передових технологій для протидії дезінформації. НАТО також вживає заходів для підвищення обізнаності громадськості щодо загроз, пов'язаних з дипфейками, та навчання людей, як розпізнавати фальшиві відео та аудіо записи. Це включає проведення тренінгів та семінарів для журналістів, громадських діячів та інших груп, які можуть бути цілями дезінформації. Крім того, НАТО співпрацює з технологічними компаніями для розробки інструментів, які допоможуть виявляти та блокувати дипфейки в реальному часі.

Штучний інтелект відіграє все більшу роль у забезпеченні інформаційної безпеки. НАТО активно використовує штучний інтелект для аналізу великих обсягів даних, виявлення аномалій та прогнозування потенційних загроз. Наприклад, у 2023 році НАТО розпочало проєкт з використання штучного інтелекту для моніторингу соціальних мереж та виявлення дезінформації. Це дозволяє швидко реагувати на нові загрози та запобігати їх поширенню. Однак використання штучного інтелекту в інформаційній безпеці також пов'язане з певними ризиками.

Одним з основних ризиків є можливість зловживання цими технологіями для маніпуляції даними та поширення дезінформації. Тому НАТО

приділяє велику увагу розробці етичних норм та стандартів для використання штучного інтелекту в інформаційній безпеці. Це включає створення прозорих та підзвітних систем, які дозволять уникнути зловживань та забезпечити захист прав людини.

Перспективи використання штучного інтелекту в інформаційній безпеці є обнадійливими, але також вимагають ретельного аналізу та врахування можливих ризиків. НАТО продовжує працювати над розробкою нових технологій та методів для покращення інформаційної безпеки, включаючи використання машинного навчання для аналізу поведінки користувачів та виявлення потенційних загроз[50].

Кібербезпека стала одним з найважливіших аспектів інформаційної безпеки в сучасному світі. Зростання кількості кібератак та їх складності вимагає постійного вдосконалення методів захисту інформації. НАТО активно працює над поліпшенням кібербезпеки своїх систем та співпрацею з країнами-членами для забезпечення захисту від кібератак. У 2024 році НАТО провело серію вправ з кібербезпеки, які дозволили оцінити готовність організації до протидії кібератакам. Ці вправи показали, що НАТО має ефективні механізми для виявлення та нейтралізації кіберзагроз, але також підкреслили необхідність подальшого вдосконалення цих механізмів. Наприклад, у 2023 році була зафіксована серія кібератак на критичну інфраструктуру в Європі, яка була успішно нейтралізована завдяки співпраці між НАТО та місцевими органами влади. Приклади успішного використання кібербезпеки в Україні та Європі показують, що ефективна співпраця та обмін інформацією є ключовими факторами для забезпечення інформаційної безпеки. НАТО продовжує вдосконалювати свої методи та технології для протидії кіберзагрозам, включаючи використання штучного інтелекту для аналізу та прогнозування кібератак[51].

Сучасні виклики інформаційної безпеки вимагають комплексного підходу та міжнародної співпраці для їх вирішення. НАТО відіграє ключову роль у забезпеченні інформаційної безпеки, використовуючи передові

технології та методи для протидії дезінформації, дипфейкам та кібератакам. Однак, незважаючи на прогрес, залишається багато роботи для подальшого вдосконалення методів та технологій інформаційної безпеки. У майбутньому НАТО повинно продовжувати вдосконалювати свої стратегії та технології для забезпечення інформаційної безпеки, враховуючи нові загрози та виклики, які виникають з розвитком технологій. Це включає розробку нових методів виявлення та протидії дезінформації, використання штучного інтелекту для аналізу та прогнозування загроз, а також співпрацю з технологічними компаніями та іншими міжнародними організаціями для забезпечення захисту інформації[52].

Розвиток технологій дипфейків та штучного інтелекту створює нові виклики для інформаційної безпеки, які вимагають комплексного підходу та міжнародної співпраці. Одним з ключових аспектів цієї проблеми є здатність швидко адаптуватися до нових загроз та розробити ефективні механізми протидії. НАТО, як провідна міжнародна організація в галузі безпеки, відіграє важливу роль у цьому процесі.

У 2025 році НАТО розпочало проєкт з розробки нових технологій для виявлення та нейтралізації дипфейків. Цей проєкт включає використання передових алгоритмів машинного навчання для аналізу відео та аудіо записів з метою виявлення ознак маніпуляції. Наприклад, завдяки цим технологіям було виявлено та нейтралізовано серію фальшивих відео, які поширювалися в соціальних мережах з метою дестабілізації ситуації в Європі. Ці відео були створені з використанням передових технологій дипфейків та мали на меті викликати паніку та недовіру серед населення. Успішне виявлення та нейтралізація цих відео підкреслює важливість використання передових технологій для забезпечення інформаційної безпеки[53].

Крім того, НАТО активно працює над розробкою нових стандартів та протоколів для забезпечення кібербезпеки. Ці стандарти включають вимоги до захисту критичної інфраструктури, обмін інформацією про кіберзагрози та співпрацю з технологічними компаніями для розробки нових інструментів

захисту. Наприклад, у 2024 році НАТО у співпраці з провідними технологічними компаніями розробило нову платформу для моніторингу кіберзагроз, яка дозволяє швидко виявляти та нейтралізувати кібератаки. Ця платформа була успішно використана для запобігання серії кібератак на критичну інфраструктуру в Європі, що підкреслює ефективність міжнародної співпраці в галузі кібербезпеки[54].

Одним з ключових аспектів роботи НАТО в галузі інформаційної безпеки є підвищення обізнаності громадськості щодо загроз, пов'язаних з дезінформацією та дипфейками. НАТО проводить регулярні тренінги та семінари для журналістів, громадських діячів та інших груп, які можуть бути цілями дезінформації. Ці заходи спрямовані на навчання людей, як розпізнавати фальшиві відео та аудіо записи, а також як захищатися від кіберзагроз. Крім того, НАТО співпрацює з освітніми установами для включення тем інформаційної безпеки до навчальних програм, що дозволяє підвищити обізнаність майбутніх поколінь щодо цих загроз[55].

НАТО також приділяє велику увагу розробці етичних норм та стандартів для використання штучного інтелекту в інформаційній безпеці. Це включає створення прозорих та підзвітних систем, які дозволять уникнути зловживань та забезпечити захист прав людини. Наприклад, у 2023 році НАТО розробило нові етичні норми для використання штучного інтелекту в військових операціях, які включають вимоги до прозорості, підзвітності та захисту особистих даних. Ці норми спрямовані на забезпечення того, що використання штучного інтелекту в інформаційній безпеці буде відповідати міжнародним стандартам та нормам.

У майбутньому НАТО повинно продовжувати вдосконалювати свої стратегії та технології для забезпечення інформаційної безпеки, враховуючи нові загрози та виклики, які виникають з розвитком технологій. Це включає розробку нових методів виявлення та протидії дезінформації, використання штучного інтелекту для аналізу та прогнозування загроз, а також співпрацю з технологічними компаніями та іншими міжнародними організаціями для

забезпечення захисту інформації. Крім того, НАТО повинно продовжувати працювати над підвищенням обізнаності громадськості щодо загроз, пов'язаних з дезінформацією та дипфейками, та навчанням людей, як захищатися від цих загроз.

Інформаційні війни, які ведуться за допомогою сучасних цифрових технологій, стали невід'ємною частиною глобальних конфліктів. НАТО, усвідомлюючи ці виклики, активно розвиває стратегії протидії гібридним загрозам, які поєднують традиційні військові дії з кібероперaціями та психологічними операціями. У 2025 році альянс представив нову концепцію "Інформаційної стійкості", яка спрямована на підвищення здатності країн-членів протистояти комплексним інформаційним операціям супротивника. Ця концепція включає створення спільних центрів моніторингу інформаційного простору, які аналізують дані з соціальних мереж, новинних ресурсів та інших цифрових платформ для виявлення ознак координованої дезінформаційної кампанії[56].

Значним кроком у цьому напрямку стало створення Центру передового досвіду з інформаційної безпеки у Талліні, який спеціалізується на аналізі кіберзагроз та розробці методів протидії інформаційним операціям. Центр проводить регулярні тренування для спеціалістів з країн-членів НАТО, навчаючи їх виявляти та нейтралізувати складні кіберзагрози. У ході одного з таких тренувань у 2024 році було виявлено та зупинено спробу масштабної атаки на інформаційні системи критичної інфраструктури кількох європейських країн. Ця подія продемонструвала ефективність колективних дій альянсу у протидії кіберзагрозам.[57].

Важливим аспектом роботи НАТО в галузі інформаційної безпеки є співпраця з приватним сектором. Альянс активно взаємодіє з провідними технологічними компаніями, такими як Microsoft, Google та Meta, для обміну інформацією про нові кіберзагрози та розробки спільних стратегій захисту. У 2025 році було підписано меморандум про співпрацю з групою технологічних компаній, який передбачає створення спільної платформи для обміну даними

про кіберінциденти та координації дій у разі масштабних кібератак. Ця співпраця дозволяє ефективніше виявляти та нейтралізувати загрози, а також розвивати нові технології захисту.

Особливу увагу НАТО приділяє захисту демократичних процесів від зовнішнього втручання. У 2024 році альянс розробив спеціальні протоколи для захисту виборчих систем від кіберзагроз та дезінформації. Ці протоколи були успішно застосовані під час виборів у кількох країнах-членах, що дозволило запобігти спробам маніпуляції виборчим процесом. Крім того, НАТО проводить регулярні навчання для виборчих комісій та політичних партій, навчаючи їх методам протидії дезінформації та кіберзагрозам.

НАТО також активно працює над розвитком технологій квантової криптографії, яка може стати ключовим елементом майбутньої інфраструктури інформаційної безпеки. У 2025 році було оголошено про запуск пілотного проєкту з використання квантових технологій для захисту комункаційних каналів альянсу. Цей проєкт спрямований на створення стійких до кібератак систем зв'язку, які зможуть забезпечити безпеку передачі даних на найвищому рівні.

У контексті зростаючої кількості кіберзагроз, НАТО продовжує розвивати свою доктрину "Кібернетичного стримування", яка передбачає використання усіх доступних засобів для запобігання кібернападів на критичну інфраструктуру країн-членів. Ця доктрина включає як захисні, так і наступальні компоненти, що дозволяє альянсу ефективно реагувати на кіберзагрози та стримувати потенційних агресорів.

У майбутньому НАТО планує посилити свої зусилля у галузі інформаційної безпеки шляхом розвитку штучного інтелекту та машинного навчання для прогнозування та запобігання кіберзагрозам. Альянс також планує розширити співпрацю з академічними установами для проведення досліджень у галузі інформаційної безпеки та підготовки кваліфікованих спеціалістів у цій сфері.

Висновки до розділу 2

Отже, розділ 2 дає змогу зрозуміти про діяльність НАТО у протидії російській дезінформації та кібератакам після 2014 року відображає комплексний підхід до забезпечення інформаційної безпеки в умовах гібридної війни, що поєднує технологічні, аналітичні та освітні заходи. Російські дезінформаційні кампанії, спрямовані на Україну та країни Центральної Європи, такі як Польща і Чехія, використовують емоційно заряджені наративи, подібні до пропаганди холодної війни, але адаптовані до цифрової епохи завдяки швидкості й масштабності сучасних платформ. Ці кампанії, від міфів про "громадянську війну" до конспірологічних теорій про "біолабораторії", створюють значні виклики для суспільної згуртованості та міжнародної підтримки України.

У відповідь НАТО через Центр стратегічних комунікацій (StratCom COE) у Ризі та Кооперативний центр кіберзахисту (CCDCOE) у Таллінні розробило ефективні механізми, включаючи моніторинг інформаційного простору, спростування фейків і навчання медіаграмотності, що дозволяють нейтралізувати дезінформацію та зміцнювати стійкість суспільств. В Україні Альянс надає технічну підтримку для захисту критичної інфраструктури, зокрема після атак, таких як NotPetya 2017 року, та сприяє інтеграції кібер- і інформаційної безпеки через спільні навчання й обмін розвідданими.

У Центральній Європі, де Росія використовує історичні упередження для підриву довіри до НАТО, Альянс успішно застосовує навчання, такі як Cyber Coalition, для відпрацювання реакції на гібридні загрози. Водночас виклики, такі як швидкість цифрових атак, вплив на російськомовне населення та потреба в більших інвестиціях у технології, вказують на необхідність постійного вдосконалення стратегій. Співпраця з ЄС, приватним сектором і громадянським суспільством, а також використання штучного інтелекту для аналізу даних і прогнозування загроз, посилюють здатність НАТО адаптуватися до мінливого характеру гібридних операцій.

Цей багатошаровий підхід, який поєднує уроки холодної війни з інноваційними методами, демонструє еволюцію Альянсу в захисті інформаційного простору та зміцненні безпеки країн-членів і партнерів.

РОЗДІЛ 3. НАПРЯМИ СПІВПРАЦІ УКРАЇНИ З НАТО В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

3.1. Трансформація інформаційного середовища в контексті розвитку технологій

Сучасне інформаційне середовище зазнає безпрецедентних змін під впливом технологічного прогресу, що суттєво трансформує способи комунікації, обробки даних і ведення інформаційних операцій. Розвиток штучного інтелекту, систем автоматичного аналізу великих даних (Big Data) та алгоритмів машинного навчання радикально змінює підхід до створення, поширення й сприйняття інформації. Якщо раніше головним ресурсом у міжнародних відносинах була військова або економічна сила, то нині вирішальним фактором стає контроль над інформаційними потоками. У цьому контексті інформаційні війни набувають нових форм — від кібератак до тонко спланованих кампаній психологічного впливу, що використовують персоналізовані алгоритми й аналітичні системи для маніпуляції громадською свідомістю[58].

Штучний інтелект дедалі частіше стає інструментом, який визначає не лише ефективність політичних комунікацій, а й масштаби впливу на міжнародну безпеку. Алгоритми ШІ здатні прогнозувати поведінку масової аудиторії, створювати адаптивний контент і навіть імітувати людську взаємодію. Використання генеративних моделей, таких як ті, що створюють тексти, зображення чи відео, відкриває простір для появи феномену deepfake — технології, яка дає змогу створювати фальсифіковані, але надзвичайно реалістичні медіа-матеріали. Це змінює характер інформаційних війн, адже фальшиві відео чи аудіо можуть бути використані для дискредитації політичних лідерів, провокування конфліктів або підриву довіри до інституцій.

Великі дані (Big Data) стають ще одним інструментом у боротьбі за інформаційне домінування. Держави й корпорації збирають мільярди одиниць інформації про користувачів — їхню поведінку, уподобання, соціальні зв’язки — і використовують це для створення точкових стратегій інформаційного

впливу. Політичні кампанії дедалі частіше будуються на аналітиці великих даних, що дозволяє точно визначати цільові групи населення, їхню сприйнятливість до певних меседжів та реакції на інформаційні подразники. Такі технології не лише посилюють ефективність комунікацій, але й створюють потенційні ризики — від маніпуляцій електоратом до підриву демократичних процесів через алгоритмічну нерівність у доступі до правдивої інформації[59].

Водночас автоматизація процесів у сфері інформаційної безпеки стає одним із ключових напрямів адаптації держав до нових викликів. Використання систем автоматичного моніторингу дозволяє у реальному часі виявляти дезінформаційні атаки, координовані інформаційні кампанії або спроби втручання у вибори. У цьому контексті країни-члени НАТО активно розвивають програми з інтеграції технологій штучного інтелекту у системи кіберзахисту. Наприклад, у межах стратегії NATO 2030 передбачено створення єдиного цифрового середовища безпеки, де інноваційні технології використовуються для виявлення, нейтралізації та прогнозування інформаційних загроз.

Особливу увагу НАТО приділяє питанням стандартизації та етичного використання нових технологій. У 2021 році Альянс ухвалив Стратегію штучного інтелекту НАТО, яка визначає принципи безпечного та прозорого впровадження ШІ у військову та інформаційну сферу. Одним із ключових завдань цієї стратегії є формування довіри між союзниками через узгоджені норми використання інтелектуальних систем, що дозволяє запобігти їхньому неконтрольованому застосуванню. Крім того, створення центрів передового досвіду з кіберзахисту та стратегічних комунікацій у країнах-членах НАТО (зокрема, у Таллінні та Ризі) свідчить про прагнення організації адаптуватися до швидких технологічних змін і формувати власну екосистему цифрової безпеки[60].

Трансформація інформаційного середовища супроводжується також розширенням можливостей для співпраці між державами, науковими установами та приватним сектором. Залучення технологічних компаній до

розробки систем кіберзахисту, аналізу даних і моніторингу соціальних мереж стало однією з ключових тенденцій останніх років. Такі партнерства сприяють підвищенню стійкості інформаційної інфраструктури країн-членів НАТО, водночас створюючи умови для розробки інноваційних механізмів реагування на гібридні загрози. У цьому контексті важливо відзначити, що розвиток технологій не лише посилює можливості оборони, а й ускладнює структуру інформаційного простору, роблячи його більш вразливим до впливу недержавних акторів, приватних компаній та навіть окремих користувачів.

Водночас поява високотехнологічних інструментів у сфері інформаційних операцій створює нову динаміку у взаємодії держав, міжнародних організацій та приватного сектору. Якщо раніше інформаційна безпека розглядалася переважно як компетенція національних урядів, то сьогодні вона вимагає багаторівневої взаємодії між усіма суб'єктами цифрової екосистеми. Приватні компанії, що володіють соціальними мережами або керують глобальними комунікаційними платформами, фактично стають політичними гравцями, здатними впливати на інформаційні процеси в межах цілих держав. Саме тому НАТО розширює партнерство з технологічними корпораціями, залучаючи їх до участі у програмах кіберспостереження, аналітики даних і розробки протоколів інформаційної безпеки.

Особливе значення має питання етичного регулювання технологічних інновацій. У ситуації, коли штучний інтелект використовується для створення автономних систем прийняття рішень, постає загроза втрати людського контролю над процесами поширення інформації. Алгоритми, створені для оптимізації комунікацій, можуть ненавмисно посилювати дезінформаційні наративи або сприяти політичній поляризації. Саме тому в межах євроатлантичного простору дедалі частіше обговорюється питання про необхідність розробки міжнародних норм щодо використання штучного інтелекту в інформаційних і військових цілях. Такі норми мають забезпечити баланс між ефективністю технологій і безпекою людини, уникнути зловживань та маніпуляцій громадською думкою через цифрові платформи.

Окремим напрямом трансформації інформаційного середовища є зростання ролі соціальних мереж у формуванні політичних рішень та міжнародного іміджу держав. Платформи, які спочатку були засобом комунікації між людьми, перетворилися на простір геополітичної конкуренції. Сучасні інформаційні війни дедалі частіше ведуться не через офіційні медіа, а через соціальні платформи, де інформація поширюється миттєво, без редакційного контролю та з мінімальними бар'єрами перевірки. Використання ботів, фейкових акаунтів, таргетованої реклами та психологічних профілів дозволяє організаторам інформаційних кампаній формувати суспільні настрої з високою точністю, створюючи ілюзію «органічного» поширення ідей. Це перетворює інформаційне поле на арену невидимого протистояння, де межа між пропагандою, маніпуляцією та публічною дипломатією стає дедалі розмитішою[61].

Важливим аспектом цієї трансформації є також швидкість еволюції інформаційних технологій, яка значно випереджає можливості політичних та військових інституцій адаптуватися до нових умов. Кіберзагрози сьогодні виникають у режимі реального часу, що потребує не лише технічної готовності, а й постійного оновлення стратегій реагування. НАТО, як провідний актор у сфері міжнародної безпеки, визнає цю проблему та активно впроваджує інноваційні моделі управління ризиками. Одним із прикладів є розвиток ініціативи NATO Innovation Fund, спрямованої на підтримку технологічних стартапів, які працюють у сфері кіберзахисту, штучного інтелекту та аналітики даних. Такі проекти покликані створити екосистему інновацій, здатну оперативно реагувати на нові виклики інформаційного простору та зміцнювати колективну стійкість Альянсу.

Сучасна епоха характеризується тим, що технології більше не є лише інструментом комунікації — вони стали самостійним чинником міжнародної політики. Контроль над інформаційними системами означає контроль над свідомістю, а отже, і над політичними процесами. У цьому контексті роль НАТО полягає не лише у забезпеченні кіберзахисту, а й у формуванні

стратегічної культури цифрової безпеки, що поєднує технологічні, етичні та політичні аспекти[62].

3.2. Інформаційна стійкість НАТО та партнерів

Питання інформаційної стійкості набуває ключового значення для збереження ефективності системи колективної безпеки НАТО в умовах гібридних загроз і цифрової турбулентності. На відміну від традиційних військових викликів, які можна визначити за конкретними ознаками, інформаційні атаки є багатовимірними, часто прихованими та розрахованими на тривалий вплив. Вони спрямовані не стільки на руйнування інфраструктури, скільки на підрив довіри — до урядів, медіа, міжнародних інституцій і навіть самого поняття правди. У цьому контексті інформаційна стійкість розглядається як здатність держави або спільноти зберігати функціональність інформаційних систем, критично мислити, протистояти дезінформаційним впливам і швидко відновлюватися після атак у цифровому середовищі.

Після 2022 року НАТО активізувало політику щодо формування спільної стратегії інформаційної стійкості. Вона ґрунтується на концепції “whole-of-society approach” — підходу, який передбачає залучення урядів, приватного сектору, наукових установ, медіа та громадянського суспільства до захисту інформаційного простору. Така модель визнає, що кібер- та інформаційні загрози не можуть бути подолані виключно військовими засобами. Наприклад, у межах Центру стратегічних комунікацій НАТО (STRATCOM COE) у Ризі активно розробляються аналітичні інструменти для виявлення маніпуляцій у соціальних мережах, аналізу трендів дезінформації та формування контрнаративів. Дослідження центру свідчать, що систематичне розвінчання фейків і створення достовірного контенту має довготривалий позитивний ефект у зміцненні довіри до офіційних джерел[63].

Водночас формування інформаційної стійкості неможливе без розвитку цифрової грамотності населення. Саме низький рівень критичного мислення є

одним із головних факторів, які роблять суспільства вразливими до зовнішніх інформаційних впливів. У цьому напрямі НАТО підтримує партнерські програми з Європейським Союзом та країнами-партнерами, зокрема Україною, Грузією, Молдовою. Ці програми спрямовані на підготовку фахівців у сфері медіаосвіти, кіберзахисту та стратегічних комунікацій. В Україні, наприклад, такі ініціативи реалізуються спільно з Центром стратегічних комунікацій при Міністерстві культури та інформаційної політики, що дозволяє ефективніше виявляти та нейтралізовувати російські інформаційні операції, спрямовані на підрив єдності суспільства.

Інформаційна стійкість також передбачає створення ефективної системи міжвідомчої координації. Одним із викликів для НАТО є різниця у рівні готовності держав-членів до реагування на кібертаки та дезінформаційні кампанії. Деякі країни, такі як Естонія, Польща чи Великобританія, мають розвинуті системи кібероборони, тоді як інші лише формують базові інституційні механізми. Для подолання цього розриву Альянс активно впроваджує політику “resilience building”, спрямовану на гармонізацію стандартів кіберзахисту, створення спільних навчальних платформ і постійне оновлення методів реагування. Одним із прикладів є навчання Cyber Coalition, що щороку відбуваються під егідою НАТО і залучають тисячі експертів з понад 30 країн. Ці навчання моделюють реальні гібридні загрози, де кібероперації супроводжуються інформаційними кампаніями, що дає змогу перевірити ефективність колективних стратегій[63].

Особливу роль у зміцненні інформаційної стійкості відіграє співпраця з технологічними компаніями та дослідницькими інститутами. НАТО визнає, що швидкість технологічних змін потребує постійного оновлення аналітичних інструментів. Для цього розвивається партнерство з приватними платформами, такими як Microsoft, Google, IBM, а також з аналітичними центрами, які спеціалізуються на виявленні дезінформації та кіберзагроз. У 2023 році НАТО започаткувало ініціативу “Defence Innovation Accelerator for the North Atlantic” (DIANA), метою якої є інтеграція інноваційних технологій — штучного

інтелекту, машинного навчання, хмарних рішень — у стратегії цифрової безпеки. Завдяки цьому Альянс прагне забезпечити технологічну перевагу у сфері інформаційних операцій і зменшити ризики, пов'язані з використанням новітніх засобів маніпуляції[60].

Разом із тим, попри значний прогрес у сфері кіберзахисту, інформаційна стійкість залишається складним і багатовимірним поняттям. Вона вимагає не лише технологічних інструментів, а й стабільної політичної волі, суспільної єдності та міждержавної довіри. Дезінформаційні атаки часто націлені саме на ці аспекти, створюючи розбіжності між союзниками або підриваючи авторитет демократичних інститутів. Тому стратегічне завдання НАТО полягає не лише у зміцненні оборонних механізмів, але й у формуванні культури інформаційної відповідальності — усвідомлення спільної ролі кожного учасника міжнародної спільноти у захисті правди, фактів і прозорості.

У цьому контексті особливої ваги набуває питання стратегії довіри — не лише до інституцій НАТО, але й між державами-членами, партнерами та громадянським суспільством. Інформаційна стійкість не може існувати у вакуумі: вона вимагає сталого діалогу, обміну розвідданими та уніфікації стандартів реагування. Упродовж останніх років Альянс розширив практику взаємного попередження про інформаційні атаки, створивши мережу оперативних контактів між національними центрами стратегічних комунікацій. Такий формат дозволяє виявляти спроби маніпулювання громадською думкою ще на ранніх етапах, до того, як вони набудуть масштабного впливу.

Важливим компонентом цієї політики стала також взаємодія з Європейським Союзом. Після 2020 року обидві організації розпочали системну координацію дій у межах Спільної декларації з кібер- та інформаційної безпеки. Вона передбачає створення спільних аналітичних груп, які займаються виявленням і класифікацією гібридних загроз. Це дозволяє поєднати оборонний потенціал НАТО з регуляторними і технологічними можливостями ЄС. Завдяки такій взаємодії формується інтегрована система інформаційного захисту, де

кожна країна може оперативно отримати підтримку у випадку масштабної атаки або кампанії дезінформації.

Особливо показовими стали результати спільних навчань та досліджень, у межах яких моделювалися сценарії гібридного втручання у виборчі процеси, інформаційний простір та функціонування державних інституцій. Наприклад, навчання “Locked Shields”, що проводяться Центром передових технологій у Таллінні, щороку перевіряють здатність країн-членів реагувати на одночасні кібертаки та хвилі дезінформації. Ці навчання виявили ключову закономірність: ефективність реагування залежить не лише від технічних ресурсів, але й від координації між структурами — урядами, медіа, військовими та громадськими організаціями. Це підкреслює, що інформаційна стійкість — це насамперед соціальний і політичний процес, а не виключно технологічний[64].

Зміцнення цієї стійкості також передбачає формування нової етики комунікації у межах демократичних суспільств. НАТО все частіше акцентує, що свобода слова та відкритість не повинні ставати вразливими точками для маніпуляцій і пропаганди. У відповідь на зростання кількості фейкових наративів Альянс розробляє концепцію “responsible communication”, яка передбачає використання прозорих і перевірених джерел, а також навчання представників державних структур правилам кризової комунікації. Цей підхід особливо актуальний у часи війни Росії проти України, коли інформаційна боротьба стала не менш важливою за військові дії на фронті.

Однак, попри помітні успіхи, перед НАТО залишається низка структурних проблем. Однією з них є розрив між технологічними можливостями провідних країн — таких як США, Великобританія, Естонія — та менш підготовленими державами, які не завжди мають достатні ресурси для реалізації складних інформаційно-аналітичних проєктів. Це створює ризик нерівномірності у загальній системі безпеки Альянсу. Іншим викликом є стрімке поширення нових деструктивних технологій — від генеративного штучного інтелекту до автономних бот-мереж, здатних масштабувати дезінформаційні кампанії протягом годин. НАТО визнає, що традиційні моделі

реагування більше не забезпечують достатньої швидкості, тому у 2024-2025 роках особлива увага приділяється автоматизації аналітичних процесів та впровадженню алгоритмів раннього попередження про інформаційні ризики[65].

Ці тенденції свідчать, що розвиток інформаційної стійкості переходить у нову фазу — від захисту до проактивного прогнозування. Альянс дедалі частіше використовує методи машинного навчання та аналізу великих даних для передбачення інформаційних загроз і визначення потенційних векторів атак. Такий підхід не лише мінімізує наслідки криз, а й дозволяє формувати стратегії довгострокової адаптації. Саме на цьому етапі НАТО поступово перетворюється з оборонного альянсу на інформаційно-аналітичну спільноту, здатну діяти на випередження, прогнозувати інформаційні кризи й вибудовувати системи колективної довіри у цифровому світі.

3.3. Прогнозні тенденції розвитку інформаційних стратегій НАТО та України в умовах гібридних загроз.

Сучасна система міжнародної безпеки дедалі більше зміщується у площину інформаційного впливу, і тому ключовим завданням НАТО у найближчі роки стане формування стратегій, орієнтованих не лише на захист, а й на випередження інформаційних загроз. Зміни у характері війни, що проявилися під час російської агресії проти України, показали, що інформаційний простір тепер є полем першого удару, а не лише допоміжним інструментом. Це вимагає від Альянсу системного переосмислення принципів стратегічних комунікацій, розвитку технологічних можливостей та створення нових стандартів реагування на інформаційні атаки.

Одним із центральних напрямів прогнозованого розвитку є глибша інтеграція технологій штучного інтелекту в системи моніторингу та аналізу інформаційних потоків. Уже сьогодні у межах NATO StratCom COE розробляються алгоритми, здатні виявляти координовані дезінформаційні

кампанії на ранніх етапах, визначаючи закономірності поширення та повторювані шаблони риторики. Протягом 2026-2029 років очікується, що ці системи будуть поєднані з платформами аналізу великих даних, що дозволить створити багаторівневу модель прогнозування інформаційних криз. Такі підходи дадуть змогу Альянсу діяти не реактивно, а проактивно, нейтралізуючи деструктивні наративи ще до того, як вони набудуть суспільного резонансу.

Паралельно прогнозується активне посилення співпраці НАТО з технологічним сектором — зокрема компаніями, що спеціалізуються на кіберзахисті, алгоритмах аналізу контенту та штучному інтелекті. Приватні технологічні корпорації володіють унікальними ресурсами для виявлення фейкових акаунтів, бот-мереж і координаційних центрів інформаційних атак. Водночас партнерство з ними несе й певні ризики, адже постає питання балансу між безпекою та свободою слова. Тому НАТО, ймовірно, зосередиться на створенні етичних рамок, що дозволять поєднувати технологічну ефективність із демократичними принципами прозорості й підзвітності.

Велика увага у прогнозах приділяється змінам у підходах до навчання та підготовки кадрів. В інформаційних війнах майбутнього перевагу матимуть не лише держави з потужними технологічними можливостями, а й ті, що володіють компетенціями у сфері аналітики, когнітивної психології, кризових комунікацій. Тому НАТО планує розширити мережу освітніх програм, де майбутні фахівці вчитимуться виявляти інформаційні атаки, аналізувати їхній вплив на суспільство та розробляти стратегії протидії. Очікується, що нові навчальні центри, зокрема у Східній Європі, відіграватимуть роль регіональних хабів з інформаційної безпеки.

Не менш важливим напрямом стане вдосконалення взаємодії між Альянсом та країнами-партнерами, насамперед Україною. Війна показала, що український досвід протидії російській пропаганді та кібератакам є унікальним джерелом практичних знань, яке НАТО активно інтегрує у власні аналітичні підходи. У наступні роки прогнозується створення спільних лабораторій та аналітичних груп, які працюватимуть над моделюванням сценаріїв

інформаційного тиску, з урахуванням українських реалій. Така співпраця зміцнює не лише обороноздатність України, а й колективну стійкість усього Альянсу.

Серед ключових викликів, які визначатимуть інформаційну політику НАТО у 2026-2029 роках, експерти називають загрозу автоматизованої дезінформації, зростання кількості deepfake-відео та інформаційну втому суспільства. Ці фактори створюють передумови для нової форми гібридних атак, де технологічний тиск поєднується з психологічним виснаженням аудиторій. У відповідь на це НАТО може перейти до формування систем «інформаційного імунітету» — довгострокових освітніх і комунікаційних програм, спрямованих на підвищення критичного мислення громадян, зміцнення довіри до офіційних джерел і зниження ефекту маніпуляції.

Ймовірно, до 2030 року стратегічна концепція НАТО включатиме окремий розділ, присвячений інформаційній безпеці як ключовому компоненту колективної оборони. Це означатиме остаточне визнання інформаційного простору не лише як додаткового елементу гібридної війни, а як самостійного фронту, на якому вирішується доля сучасних конфліктів. Таке переосмислення змінить архітектуру безпеки в усьому євроатлантичному просторі, визначаючи інформаційний вимір як головну арену стратегічного суперництва між демократіями та авторитарними режимами.

Висновки до розділу 3

Отже, розділ 3 дослідив що, сучасне інформаційне середовище дедалі більше набуває ознак динамічної, технологічно насиченої системи, у якій межі між правдою, маніпуляцією та алгоритмічно сконструйованою реальністю поступово стираються. Розвиток штучного інтелекту, технологій обробки великих даних і автоматизованих систем комунікації не лише змінив саму структуру інформаційного обміну, а й суттєво вплинув на характер міжнародних відносин. У глобальному масштабі відбувається перехід від

традиційної боротьби за ресурси до боротьби за інформаційний вплив, де основним полем протистояння стають цифрові простори та свідомість громадян.

Використання новітніх технологій у політичних і військових цілях формує нові типи загроз, які важко передбачити або ідентифікувати традиційними методами безпеки. Штучний інтелект і алгоритмічні системи не лише оптимізують процеси аналізу даних, але й створюють умови для більш витончених форм дезінформації, які здатні змінювати суспільні настрої та впливати на політичні рішення. Саме тому у сучасному міжнародному середовищі інформаційна безпека вже не може розглядатися як окремий елемент оборони — вона стає фундаментом державної та міждержавної стабільності.

У цьому контексті роль НАТО набуває якісно нового виміру. Альянс поступово трансформується з військово-політичного союзу у багаторівневу платформу безпеки, де технологічні, аналітичні та гуманітарні інструменти взаємодіють у межах єдиного стратегічного підходу. Його діяльність у сфері цифрової безпеки свідчить про усвідомлення того, що майбутні конфлікти розгортатимуться не лише на полі бою, а й у віртуальному просторі, де перемогу здобуває не той, хто має більше зброї, а той, хто краще контролює інформаційні потоки.

Отже, трансформація інформаційного середовища під впливом технологій вимагає не лише технічних рішень, а й глибокого переосмислення ціннісних та етичних засад міжнародної взаємодії. Уміння поєднати інноваційність із відповідальністю, технологічний прогрес — із прозорістю та довірою, стає вирішальним фактором стабільності у світі, де інформація перетворилася на найпотужнішу зброю XXI століття.

ВИСНОВКИ

Проведене дослідження підтвердило, що роль НАТО у забезпеченні інформаційної безпеки в умовах гібридних загроз є системною та багатошаровою. Теоретичний аналіз виявив, що основу діяльності Альянсу формують концепції інформаційної війни, інформаційного домінування, гібридних загроз та когнітивної безпеки. З'ясовано еволюцію підходів НАТО: від ідеологічного протистояння часів холодної війни через визнання кіберпростору окремим операційним доменом (Варшавський саміт 2016) до сучасної парадигми когнітивної війни та інформаційної стійкості (2021-2025).

Проведене дослідження дозволило виконати всі поставлені завдання та сформулювати такі висновки:

1. Теоретичну основу діяльності НАТО у сфері інформаційної безпеки формують концепції інформаційної війни, інформаційного домінування, гібридних загроз, когнітивної війни та когнітивної стійкості. Сучасний етап характеризується розумінням когнітивної сфери як самостійного виміру конфлікту, де головною мішенню є свідомість, сприйняття та процеси прийняття рішень людини і суспільства.

2. Еволюція теоретичних підходів НАТО пройшла такі ключові етапи: - період Холодної війни - ідеологічне протистояння та психологічні операції; - 1991-2014 - акцент на миротворчість і боротьбу з тероризмом; - після 2014 - визнання гібридної війни як основної загрози; - 2016 (Варшавський саміт) - проголошення кіберпростору п'ятим операційним доменом; - 2021-2025 - перехід до парадигми когнітивної війни та побудови інформаційної стійкості суспільства.

3. Ключовими доктринальними документами є Стратегічна концепція 2022 року, оновлена Політика кіберзахисту, Стратегія штучного інтелекту НАТО (2021, оновлена 2024) та Концепція когнітивної війни (NATO ACT, 2021). Їх практична реалізація забезпечується через спеціалізовані центри StratCom COE (Рига), CCDCOE (Таллінн) і Hybrid CoE (Гельсінкі).

4. З 2014 року НАТО відіграє активну роль у протидії російській дезінформації проти України шляхом моніторингу та спростування кремлівських наративів (тісна координація з EUvsDisinfo), підтримки медіаграмотності, публічних атрибуцій і створення у 2022 році Українського офісу зв'язків зі стратегічними комунікаціями НАТО. У кіберсфері Альянс забезпечує навчання (Cyber Coalition, Locked Shields), технічну допомогу після атак NotPetya, WhisperGate та масштабних DDoS 2022-2025 рр., повноправне членство України в CCDCOE (2024) та застосування положень Tallinn Manual 2.0 і 3.0.

5. Аналіз кейсів іноземного втручання у демократичні вибори та референдуми після 2016 року (США 2016, Франція 2017, Німеччина 2017, Європарламент 2019, численні кампанії 2020-2025) дозволив запропонувати такі рекомендації для посилення ролі НАТО: - створити при SHAPE спеціалізований Центр протидії іноземному втручанню у демократичні процеси; - запровадити для всіх держав-членів систему швидкого реагування Rapid Alert System (24-48 годин); - розширити програми пре-банкінгу та інокуляції населення, активно використовуючи український досвід 2014-2025 рр.; - прискорити розгортання ШІ-інструментів для автоматичного виявлення deepfake-контенту та бот-мереж у реальному часі; - інституціоналізувати обмін українським досвідом через створення постійно діючого NATO-Ukraine Hybrid Warfare Training Hub.

Отже, НАТО сформувало цілісну доктринальну, інституційну та практичну систему протидії гібридним загрозам в інформаційному та когнітивному просторах. Подальше посилення цієї системи має відбуватися через глибшу інтеграцію унікального українського досвіду протидії російській гібридній агресії та прискорене впровадження технологій штучного інтелекту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. How the US and Europe can counter Russian information manipulation about nonproliferation . Atlantic Council. URL: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/how-the-us-and-europe-can-counter-russian-information-manipulation-about-nonproliferation/ (date of access: 06.10.2025).

2. Cyber Defence. NATO. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm (date of access: 06.10.2025).

3. The Future of Information Warfare: AI and Cognitive Security . Brookings Institution, 2025. URL: https://www.brookings.edu/articles/artificial-intelligence-international-security-and-the-risk-of-war/ (date of access: 06.10.2025).

4. THE INFORMATIONAL DIMENSION OF HYBRID WARFARE . CENSS. URL: https://censs.org/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D0%B9-%D0%B2%D0%B8%D0%BC%D1%96%D1%80-%D0%B3%D1%96%D0%B1%D1%80%D0%B8%D0%B4%D0%BD%D0%BE%D1%97-%D0%B2%D1%96%D0%B9%D0%BD%D0%B8/?lang=en (date of access: 07.10.2025).

5. Redefining Hybrid Warfare: Russia’s Non-linear War against the West . Journal of Strategic Security, 2017. Vol. 10, № 1, P. 17-31. URL: https://www.researchgate.net/publication/316637417_Redefining_Hybrid_Warfare_Russia's_Non-linear_War_against_the_West (date of access: 07.10.2025).

6. Hybrid Threats: The Baltic Perspective . CSCE. URL: https://www.csce.gov/wp-content/uploads/2022/03/RKols_Hybrid-threats-Baltic-Perspective-2022.pdf (date of access: 07.10.2025).

7. Khaldarova, I., Pantti, M. Fake News: The Narrative Battle over the Ukrainian Conflict . Journalism Practice, 2023. URL: https://www.academia.edu/24362058/Fake_News_The_narrative_battle_over_the_Ukrainian_conflict (date of access: 07.10.2025).

8. Knowledge security: insights for NATO . NATO Review. URL: https://www.nato.int/docu/review/articles/2022/09/30/knowledge-security-insights-for-nato/index.html (date of access: 08.10.2025).

9. NATO Cyber Security Centre . NCIA. URL: https://www.ncia.nato.int/about-us/newsroom/nato-cyber-security-centre-experiments-with-secure-network-capable-of-withstanding-attack-by-quantum-computers (date of access: 08.10.2025).

10. AI, Media Literacy, and the Next Generation . Eurozine. URL: https://www.eurozine.com/ai-media-literacy-and-the-next-generation/ (date of access: 08.10.2025).

11. Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept . *Frontiers in Big Data*, 2024. URL: https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1452129/full (date of access: 08.10.2025).

12. Fake History: How Russia Manipulates Ukraine's Past . *UkraineWorld*. URL: https://ukraineworld.org/en/articles/analysis/russia-manipulates-ukraines-past (date of access: 09.10.2025).

13. NATO's approach to counter hybrid threats . NATO. URL: https://www.nato.int/cps/ru/natohq/topics_219728.htm?selectedLocale=en (date of access: 09.10.2025).

14. Cognitive Warfare . NATO ACT. URL: https://www.act.nato.int/activities/cognitive-warfare/ (date of access: 09.10.2025).

15. NATO Strategy Documents 1949-1969 . NATO. URL: https://www.nato.int/docu/stratdoc/eng/intro.pdf (date of access: 09.10.2025).

16. CIA Analysis of the Warsaw Pact Forces . CIA Reading Room. URL: https://www.cia.gov/readingroom/ (date of access: 10.10.2025).

17. NATO's "shield" helps nations thrive . *ShareAmerica*. URL: https://share.america.gov/nato-s-shield-helps-nations-thrive/ (date of access: 10.10.2025).

18. Soviet Subversion, Disinformation and Propaganda: How the West Fought Against it . LSE, 2018. URL: https://www.lse.ac.uk/iga/assets/documents/arena/2018/Jigsaw-Soviet-Subversion-Disinformation-and-Propaganda-Final-Report.pdf (date of access: 10.10.2025).

19. What's Old Is New Again: Cold War Lessons for Countering Disinformation . *Texas National Security Review*, 2022. URL: https://tnsr.org/2022/09/whats-old-is-new-again-cold-war-lessons-for-countering-disinformation/ (date of access: 10.10.2025).

20. Стратегічна концепція НАТО 2022 . NATO, 2022. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf (дата звернення: 11.10.2025).

21. Brussels Summit Communiqué 2018 . NATO, 2018. URL: https://otan.delegfrance.org/Brussels-Summit-Communique-2018 (date of access: 11.10.2025).

22. Hybrid CoE . Hybrid CoE. URL: https://www.hybridcoe.fi/ (date of access: 11.10.2025).

23. Warsaw Summit Communiqué . NATO. URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm (date of access: 11.10.2025).

24. Does the New EU-NATO Joint Declaration Matter? . CSIS. URL: https://www.csis.org/analysis/does-new-eu-nato-joint-declaration-matter (date of access: 12.10.2025).

25. ANALYSIS OF RUSSIA'S INFORMATION CAMPAIGN AGAINST UKRAINE . NATO Strategic Communications Centre of Excellence. URL: https://stratcomcoe.org/cuploads/pfiles/russian_information_campaign_public_12012016fin.pdf (date of access: 12.10.2025).

26. Russian propaganda stoke anti-Ukraine sentiment and misinform across the region . Visegrad Info. URL: https://visegradinfo.eu/index.php/collaborative/668-russian-propaganda-stoke-anti-ukraine-sentiment-and-misinform-across-the-region (date of access: 12.10.2025).

27. Mapping Russian Disinformation Narratives and Their Impact Across Europe in the Face of the 2024 European Parliament Election . Center for European Policy Analysis. URL: https://natoassociation.ca/mapping-russian-disinformation-narratives-and-their-impact-across-europe-in-the-face-of-the-2024-european-parliament-election/ (date of access: 12.10.2025).

28. Internet Trolling as a hybrid warfare tool: the case of Latvia . NATO Strategic Communications Centre of Excellence. URL: https://stratcomcoe.org/publications/internet-trolling-as-a-hybrid-warfare-tool-the-case-of-latvia/160 (date of access: 13.10.2025).

29. NATO StratCom Dialogue . NATO Strategic Communications Centre of Excellence. URL: https://rigastratcomdialogue.org/ (date of access: 13.10.2025).

30. Питання та відповіді щодо East StratCom Task Force . Європейська служба зовнішньої діяльності. URL: https://europa.eu/rapid/press-release_MEMO-18-6648_en.htm (дата звернення: 13.10.2025).

31. NATO's approach to counter information threats . NATO. URL: https://www.nato.int/cps/en/natolive/topics_219728.htm (date of access: 13.10.2025).

32. Course Catalogue 2023 . NATO Communications and Information Systems School, 2023. URL: https://www.nordefco.org/files/NORDEFCO_2023_COURSE_CATALOGUE.pdf (date of access: 14.10.2025).

33. Протидіємо безперервним дезінформаційним кампаніям Росії: вісім років роботи EUvsDisinfo . EUvsDisinfo, 2023. URL: https://euvsdisinfo.eu/to-challenge-russias-ongoing-disinformation-campaigns-eight-years-of-euvsdisinfo/ (дата звернення: 14.10.2025).

34. RUSSIAN INFORMATION WARFARE IN CENTRAL AND EASTERN EUROPE: STRATEGIES, IMPACT, COUNTERMEASURES . German Marshall Fund of the United States, 2019. URL: https://www.gmfus.org/sites/default/files/Russia%20disinformation%20CEE%20-%20June%204.pdf (date of access: 14.10.2025).

35. Лідери країн НАТО схвалили комплексну політику кіберзахисту альянсу. Інтерфакс-Україна, 2021. URL: https://interfax.com.ua/news/general/750063.html (дата звернення: 14.10.2025).

36. Цифровізація та кібербезпека: пріоритети для України та НАТО . Україна-НАТО, 2023. URL: https://ukrainetonato.com.ua/75-rokiv-nato/tsyfrovizatsiia-ta-kiberbezpeka-priorytety-dlia-ukrainy-ta-nato/ (дата звернення: 15.10.2025).

37. US widens indictment of Russians in ‘WhisperGate’ conspiracy to destroy Ukrainian and NATO systems . AP News, 2025. URL: https://apnews.com/article/russian-cyberattacks-whispergate-indictments-doj-fbi-1430724940a2f7732158e3512ac2a881 (date of access: 15.10.2025).

38. NATO Faces Russian Provocations via Drone Activity and Disinformation: A Necessary Western Response . DISA, 2025. URL: https://disa.org/nato-faces-russian-provocations-via-drone-activity-and-disinformation-a-necessary-western-response/ (date of access: 15.10.2025).

39. Ukraine to be accepted as a Contributing Participant to NATO CCDCOE . NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2023. URL: https://ccdcoe.org/news/2022/ukraine-to-be-accepted-as-a-contributing-participant-to-nato-ccdcoe/ (date of access: 15.10.2025).

40. Фахівці Міноборони та Збройних Сил України з питань кібербезпеки відвідали структури НАТО . АрміяInform, 2023. URL: https://armyinform.com.ua/2023/07/10/fahivczi-minoborony-ta-zbrojny Ones-syl-ukrayiny-z-pytan-kiberbezpeky-vidvidaly-struktury-nato/ (дата звернення: 16.10.2025).

41. Countering Disinformation: NATO’s Role in Building Resilience . NATO Review, 2024. URL: https://www.napforum.org/policy-briefs/nato-s-shield-countering-disinformation-on-defense-investment (date of access: 16.10.2025).

42. Poland identifies Russian group allegedly aiming to sway elections, deputy PM says . Reuters, 2025. URL:

https://www.reuters.com/world/europe/poland-identifies-russian-group-allegedly-aiming-sway-elections-deputy-pm-says-2025-01-10/ (date of access: 16.10.2025).

43. Cyber Coalition 2024: Strengthening NATO's Cyber Defence . JFC Brunssum, 2024. URL: https://jfcbs.nato.int/page5964943/2024/cyber-coalition-2024--strengthening-natocyber-defence (date of access: 16.10.2025).

44. Poland Strengthens Cybersecurity Cooperation with NATO Amid Rising Hybrid Threats . *International Finance*, 2024. URL: https://internationalfinance.com/economy/if-insights-how-polands-resilience-strategy-benefits-europe/ (date of access: 17.10.2025).

45. Czech Republic Enhances Cyber Resilience Through NATO's CCDCOE Initiatives . CyberDefence News, 2024. URL: https://ccdcoe.org/library/publications/national-cyber-security-organisation-czech-republic/ (date of access: 17.10.2025).

46. Огляд подій у сфері кібербезпеки, лютий 2024 . Рада національної безпеки і оборони України, Київ, 2024. URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/Cyber%20digest%2002_2024/Cyber%20digest_Fab_2024_UA.pdf (дата звернення: 17.10.2025).

47. Річний аналітичний огляд: ключові події, тенденції та виклики у сфері кібербезпеки у 2024 році . Рада національної безпеки і оборони України, Київ, 2024. URL: https://www.rnbo.gov.ua/ua/Diialnist/7095.html (дата звернення: 17.10.2025).

48. Deepfakes in warfare: new concerns emerge from their use around the Russian invasion of Ukraine . *The Conversation*, 2025. URL: https://theconversation.com/deepfakes-in-warfare-new-concerns-emerge-from-their-use-around-the-russian-invasion-of-ukraine-216393 (date of access: 18.10.2025).

49. Summary of NATO's revised Artificial Intelligence (AI) strategy . NATO, 2024. URL: https://www.nato.int/cps/en/natohq/official_texts_227237.htm (date of access: 18.10.2025).

50. NATO Allies join forces to enhance the security of critical undersea infrastructure . NATO, 2024. URL: https://www.nato.int/cps/en/natohq/news_231270.htm (date of access: 18.10.2025).

51. NATO AND AI - REPORT 2024 . NATO Parliamentary Assembly, 2024. URL: https://www.nato-pa.int/document/2024-nato-and-ai-report-clement-058-stc (date of access: 18.10.2025).

52. How Reality Defender Exposed Political Misinformation in a Leading NATO Country . *Reality Defender*, 2025. URL: https://www.realitydefender.com/case-studies/how-reality-defender-exposed-political-misinformation-in-a-leading-nato-country (date of access: 19.10.2025).

53. The Potential of NATO's Cybersecurity Proposals . *SecureWorld*, 2025. URL: https://www.secureworld.io/industry-news/potential-nato-cybersecurity-proposal (date of access: 19.10.2025).

54. NATO-EU cooperation on countering disinformation . NATO, 2024. URL: https://www.nato.int/cps/en/natohq/topics_132722.htm (date of access: 19.10.2025).

55. Algorithmic invasions: How information warfare threatens NATO's eastern flank . *NATO Review*, 2025. URL: https://www.nato.int/docu/review/articles/2025/02/07/algorithmic-invasions-how-information-warfare-threatens-natos-eastern-flank/index.html (date of access: 20.10.2025).

56. World's most advanced cyber defence exercise kicks off in Tallinn . NATO CCDCOE, 2024. URL: https://ccdcoe.org/news/2024/worlds-most-advanced-cyber-defence-exercise-kicks-off-in-tallinn/ (date of access: 20.10.2025).

57. Unlocking the power of machine learning in big data . *ScienceDirect*, 2025. URL: https://www.sciencedirect.com/science/article/pii/S2666764925000104 (date of access: 20.10.2025).

58. Pauwels, E. Preparing for Next-Generation Information Warfare with Generative AI . *Center for International Governance Innovation*, 2024. URL:

https://www.cigionline.org/static/documents/Pauwels-Nov2024.pdf (date of access: 20.10.2025).

59. Summary of NATO's revised Artificial Intelligence (AI) strategy . NATO, 2024. URL: https://www.nato.int/cps/en/natohq/official_texts_227237.htm (date of access: 20.10.2025).

60. How AI Threatens Democracy . *Journal of Democracy*, 2025. URL: https://www.journalofdemocracy.org/articles/how-ai-threatens-democracy/ (date of access: 20.10.2025).

61. The Polarizing Impact of Political Disinformation and Hate Speech on Social Media . PMC, 2023. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC10106894/ (date of access: 20.10.2025).

62. Social Media Manipulation 2022/2023: Assessing the Ability of Social Media Companies to Combat Platform Manipulation . NATO Strategic Communications Centre of Excellence, 2023. URL: https://stratcomcoe.org/publications/social-media-manipulation-20222023-assessing-theability-of-social-media-companies-to-combat-platform-manipulation/272 (date of access: 20.10.2025).

63. Cyber Deterrence in the Age of AI: How NATO is Adapting to Intelligent Threats from Russia and China . New Geopolitics Research Network, 2025. URL: https://www.newgeopolitics.org/2025/05/28/cyber-deterrence-in-the-age-of-ai-how-nato-is-adapting-to-intelligent-threats-from-russia-and-china/ (date of access: 20.10.2025).

64. Virtual Manipulation Brief 2025 . NATO Joint Analysis and Lessons Learned Centre, 2025. URL: https://nllp.jallc.nato.int/iks/sharing%20public/vmb-final-8325b.pdf (date of access: 20.10.2025).

АНОТАЦІЯ

Котляров М.А. НАТО у забезпеченні інформаційної безпеки в умовах гібридних загроз (магістерська робота). Харків, ХНУ імені В.Н. Каразіна, 2025р.

Кваліфікаційна робота магістра присвячена дослідженню ролі НАТО у забезпеченні інформаційної безпеки в умовах гібридних загроз; з'ясовано теоретичні засади діяльності Альянсу у сфері інформаційної та когнітивної безпеки; визначено зміст та особливості сучасних гібридних загроз, що поєднують інформаційні, кібернетичні та психологічні методи впливу; здійснено оцінку стратегічних підходів НАТО до протидії дезінформації, кібератакам і маніпулятивним інформаційним кампаніям після 2014 року; досліджено практичні інструменти, такі як діяльність Центру передового досвіду зі стратегічних комунікацій (StratCom COE), а також ініціативи з кіберзахисту та підвищення стійкості країн-членів і партнерів; визначено вплив гібридних загроз на інформаційний простір України та держав Балтії; охарактеризовано механізми підтримки України, включаючи обмін даними, протидію російській дезінформації та реагування на кібератаки; здійснено аналіз ефективності стратегій НАТО та визначено проблеми й потреби їх удосконалення.

Ключові слова: НАТО, інформаційна безпека, гібридні загрози, дезінформація, кібербезпека, StratCom COE, Росія, Україна, стратегічні комунікації.

ANNOTATION

Kotliarov M.A. *NATO in Ensuring Information Security under Hybrid Threats* (Master's Thesis). Kharkiv: V. N. Karazin Kharkiv National University, 2025.

The master's qualification work is devoted to the study of NATO's role in ensuring information security in the context of hybrid threats; the theoretical foundations of the Alliance's activities in the field of information and cognitive security are clarified; the content and specific features of modern hybrid threats that combine informational, cyber and psychological methods of influence are defined; an assessment of NATO's strategic approaches to countering disinformation, cyberattacks and manipulative information campaigns after 2014 has been carried out; practical instruments such as the work of the Strategic Communications Centre of Excellence as well as initiatives on cybersecurity and resilience-building for member and partner states, are studied; the impact of hybrid threats on the information space of Ukraine and the Baltic states is determined; mechanisms of NATO's support for Ukraine, including information exchange, countering Russian disinformation, and responding to cyberattacks, are characterized;

Keywords: NATO, information security, hybrid threats, disinformation, cybersecurity, StratCom COE, Russia, Ukraine, strategic communications.

ВІДГУК
на кваліфікаційну роботу магістра
студента 2-го курсу групи УМІБ-61 денної форми навчання
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
освітньо-професійної програми «Міжнародна інформаційна безпека»
Навчально-наукового інституту «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В. Н. Каразіна
Котлярова Максима Артемовича
на тему: «НАТО у забезпеченні інформаційної безпеки в умовах гібридних загроз»

Магістерська кваліфікаційна робота Котлярова Максима Артемовича присвячена комплексному дослідженню ролі НАТО в інформаційній безпеці в умовах сучасних гібридних загроз. Актуальність теми зумовлена посиленням інформаційного протистояння, зростанням масштабів дезінформації та кібератак, а також активним використанням когнітивних інструментів впливу у міжнародних конфліктах, що визначає стратегічне значення інформаційної безпеки для держав-членів НАТО і партнерів, зокрема України.

Робота має чітку структуру і складається зі вступу, трьох розділів, висновків та списку використаних джерел. У першому розділі проаналізовано теоретичні засади діяльності НАТО в інформаційній сфері, розкрито концепцію гібридних загроз і показано еволюцію поглядів Альянсу на природу інформаційних конфліктів. У другому розділі детально розглянуто діяльність НАТО щодо протидії російській дезінформації і кіберактивності, наведено приклади інформаційних операцій проти України та країн Балтії, а також проаналізовано заходи НАТО з кіберзахисту та стратегічних комунікацій. Третій розділ присвячено перспективам поглиблення співпраці України з НАТО в сфері інформаційної безпеки, визначено пріоритетні напрямки розвитку, зокрема посилення інформаційної стійкості, розширення міжнародних програм, впровадження медіаграмотності та застосування сучасних технологій штучного інтелекту для виявлення дезінформації.

Оцінка отриманих результатів свідчить, що автор успішно реалізував поставлену мету і завдання. Робота містить обґрунтований аналіз інструментів протидії гібридним інформаційним загрозам і продемонстровано комплексний підхід до розуміння політики НАТО у сфері інформаційної безпеки. Представлені висновки узгоджуються з емпіричними матеріалами та сучасною практикою діяльності Альянсу, а сформульовані рекомендації для України мають прикладний характер і відповідають актуальним потребам державної інформаційної політики.

Водночас було б доцільно більш розгорнуто представити критерії оцінки ефективності програм стратегічних комунікацій НАТО та надати порівняльний аналіз практик різних країн-членів Альянсу. Таке уточнення дозволило б підсилити прикладну частину роботи, однак зауваження носить рекомендаційний характер і не впливає на загальну позитивну оцінку результатів дослідження.

Магістерська кваліфікаційна робота Котлярова Максима Артемовича відповідає основним критеріям, установленим для випускних досліджень другого (магістерського) рівня вищої освіти. Дослідження характеризується змістовною завершеністю, належною аргументацією висновків, коректним використанням теоретичних підходів і здатністю автора формувати практично орієнтовані пропозиції. Робота відображає самостійність наукового пошуку здобувача та може бути представлена до розгляду і захисту перед екзаменаційною комісією.

Науковий керівник:
д. держ. упр., професор,
професор кафедри міжнародних відносин Солових В. П.

РЕЦЕНЗІЯ

на кваліфікаційну роботу магістра
студента 2-го курсу групи УМІБ-61 денної форми навчання
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
освітньо-професійної програми «Міжнародна інформаційна безпека»
Навчально-наукового інституту «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В.Н. Каразіна
Котлярова Максима Артемовича
на тему: «НАТО у забезпеченні інформаційної безпеки в умовах гібридних загроз»

1. Актуальність теми

Магістерська робота присвячена надзвичайно актуальній та науково значущій темі, що безпосередньо стосується сучасної архітектури міжнародної безпеки, розвитку гібридних форм протистояння та ролі інформаційних стратегій у діяльності НАТО. У контексті повномасштабної російсько-української війни розгляд механізмів протидії дезінформації та зміцнення інформаційної стійкості набуває особливої практичної ваги, що безсумнівно підсилює актуальність дослідження.

Проблематика забезпечення інформаційної безпеки в умовах зростання гібридних загроз набуває визначального значення для системи євроатлантичної безпеки. Російські інформаційні та кібероперації, спрямовані проти України, держав-членів НАТО та партнерів, продемонстрували вразливість демократичних інституцій перед скоординованими дезінформаційними кампаніями, операціями впливу та атаками на критичну інфраструктуру.

У цьому контексті системний аналіз ролі НАТО як ключового безпекового актора є своєчасним та обґрунтованим. Робота поєднує огляд доктринальних документів Альянсу, оцінку практичних механізмів реагування і виявлення чинників, що обумовлюють ефективність протидії гібридним загрозам.

2. Характеристика якості виконання розділів роботи

Зміст розділів продемонстрував уміння автора систематизувати матеріал, вибудовувати аргументацію та використовувати релевантні джерела. Робота має чітку логічну структуру: складається зі вступу, трьох розділів, висновків та

списку використаних джерел (64 позиції), що відповідає вимогам до кваліфікаційних робіт магістерського рівня.

У першому розділі автор розкриває теоретичні та концептуальні засади інформаційної безпеки в контексті діяльності НАТО. На основі сучасних стратегічних документів (Стратегічна концепція 2022 року, Брюссельська декларація, матеріали StratCom COE тощо) визначено еволюцію підходів та інституційні механізми реагування на гібридні виклики. Матеріал подано системно, з опорою на актуальні джерела, що свідчить про достатній ступінь теоретичної підготовки автора.

Другий розділ присвячено аналізу протидії НАТО російській дезінформації та кіберзагрозам після 2014 року. Автор якісно опрацьовує конкретні кейси гібридних атак, наводить приклади операцій, дезінформаційних кампаній та заходів Альянсу у відповідь. Позитивним є поєднання роботи з відкритими аналітичними звітами, матеріалами міжнародних дослідницьких центрів (Brookings Institution, CEPA, CENSS), що забезпечує високий рівень емпіричної достовірності.

У третьому розділі розглянуто напрями співпраці України з НАТО у сфері інформаційної безпеки. Автор аналізує перспективи впровадження ШІ, розвиток систем раннього виявлення загроз, формування інформаційної стійкості та прогнозує трансформацію стратегічних підходів НАТО до 2030 року. Розділ має вагоме практичне спрямування та містить конкретні рекомендації, які можуть бути використані в діяльності українських державних структур і партнерських інституцій.

3. Ступінь обґрунтованості висновків

Висновки роботи є логічними та аргументованими. Вони відповідають змісту розділів і відображають ключові результати аналітичної роботи. Автор чітко формулює висновки про роль НАТО в інформаційній безпеці та необхідність зміцнення можливостей України як полігону гібридних випробувань та джерела унікального досвіду для НАТО. Практичне значення роботи полягає в можливості застосування отриманих результатів у сферах міжнародної безпеки, стратегічних комунікацій, державної інформаційної політики та освітніх програм, а також для експертних розробок у сфері протидії дезінформації.

4. Позитивні сторони роботи

Робота вирізняється чіткістю структури, виваженим підходом до аналізу джерел. Автор широко використовує сучасну термінологію, аналітичні

матеріали та актуальні концепції інформаційної війни.. Привертає увагу спроба структурування сучасних гібридних загроз та їхнього впливу на держави-члени й партнерів Альянсу, а також поєднання кейс-методу з елементами прогнозного аналізу.

5. Недоліки роботи

Серед недоліків відмітимо обмежене висвітлення внутрішніх дискусій у межах НАТО та недостатнє опрацювання ролі приватних цифрових платформ у інформаційних операціях. У деяких фрагментах бажано поглибити критичний аналіз наявних досліджень, оскільки часом автор обмежується дескрипцією. Однак ці зауваження не зменшують загальної якості дослідження.

6. Загальна оцінка кваліфікаційної роботи

Кваліфікаційна робота Котлярова Максима Артемовича відповідає вимогам, встановленим до магістерських досліджень спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії». Дослідження має практичну релевантність та демонструє здатність автора до самостійного аналізу.

Рецензент:
кандидат соціологічних наук (доктор філософії),
доцент кафедри соціально-гуманітарних наук
Харківського національного університету
міського господарства імені О. М. Бекетова Олександра ЗІНЧИНА

Підпис О. Зінчина
Засвідчую:
ст. інспектор відд. кадрів
"____" _____ 20__ р.