МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
ФАКУЛЬТЕТ ПРАВА ТА МІЖНАРОДНИХ ВІДНОСИН

Кафедра міжнародних відносин

Спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»

Освітня програма 291.00.01 «Суспільні комунікації»

БАКАЛАВРСЬКА РОБОТА
на тему:
ІНСТРУМЕНТИ ТА МЕХАНІЗМИ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ НАТО В УМОВАХ СУЧАСНИХ ЗАГРОЗ

Студентки 4 курс
денної форми навчання
Папян Соломії Йосипівни

Науковий керівник:
канд. політ. наук,
доцент кафедри міжнародних відносин
Караваєв В.С.

Київ – 2026

ЗМІСТ

ВСТУП

Актуальність теми дослідження зумовлена зростанням ролі інформаційного чинника у сучасних конфліктах та посиленням гібридних форм протистояння між державами. Інформаційні кампанії, дезінформаційні операції та маніпулятивні наративи здатні впливати на політичні рішення, підривати довіру до державних інституцій та дестабілізувати суспільства. У цьому контексті НАТО приділяє значну увагу розвитку інструментів стратегічних комунікацій, інформаційної безпеки та протидії дезінформації. Дослідження механізмів реалізації інформаційної політики Альянсу дозволяє краще зрозуміти роль інформаційного виміру у системі міжнародної безпеки та визначити ефективні підходи до протидії сучасним загрозам.

Об'єктом дослідження є інформаційна політика НАТО як складова системи міжнародної безпеки.

Предметом дослідження виступають інструменти та механізми реалізації інформаційної політики НАТО в умовах сучасних інформаційних та гібридних загроз.

Метою дослідження є встановлення інструментів і механізмів реалізації інформаційної політики НАТО та визначення їхньої ролі у протидії сучасним інформаційним викликам.

Для досягнення поставленої мети визначено такі ***завдання дослідження:***

- дослідити стан наукової розробки проблеми та джерельну базу дослідження;
- розкрити понятійно-категоріальний апарат та методи дослідження;
- охарактеризувати інституційну структуру та ключові напрями інформаційної діяльності Альянсу;
- визначити основні інформаційні та гібридні загрози у сучасному міжнародному середовищі;

- проаналізувати роль дезінформації, пропаганди та інформаційних операцій як інструментів впливу;
- дослідити інструменти стратегічних комунікацій та цифрових платформ у реалізації інформаційної політики НАТО;
- оцінити роль співпраці НАТО з державами-членами та партнерами у сфері інформаційної безпеки.

Теоретичне значення дослідження полягає у поглибленні наукового розуміння інформаційної політики міжнародних організацій та її ролі у сучасній системі міжнародної безпеки.

Практичне значення роботи полягає у можливості використання отриманих результатів у подальших дослідженнях проблем міжнародної інформаційної безпеки, стратегічних комунікацій та протидії інформаційним загрозам, а також у навчальному процесі під час вивчення дисциплін, пов’язаних із міжнародними відносинами та безпековими студіями.

Структура роботи зумовлена метою та завданнями дослідження. Робота складається зі вступу, трьох розділів, висновків та списку використаних джерел і літератури. У роботі наведено 4 рисунки, 8 таблиць, використано 71 джерело. Основний обсяг роботи становить 68 сторінки.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ НАТО

1.1. Стан наукової розробки проблеми та джерельна база дослідження

Поняття інформаційної політики сформувалося у наукових дослідженнях 60–70-х років XX століття та описувало нову політичну, правову, соціально-економічну й технологічну систему обміну інформацією. Вона ґрунтувалася на інституційних механізмах реалізації цієї політики та на передових досягненнях інформаційних технологій.

У межах ідеології інформаційного суспільства існують різні підходи, напрями й тенденції, що розглядають нові соціальні перспективи. До них належать як позитивні можливості – ефективніше державне управління економікою та формування законодавчої бази для вільного доступу й обміну інформацією між державами та громадянами, – так і потенційні ризики, пов’язані з інформаційною безпекою міжнародного інформаційного обміну та необхідністю правового врегулювання можливих конфліктів.[1]

Інформаційна політика є специфічною сферою суспільної діяльності, пов’язаною зі створенням, відтворенням і поширенням інформації, яка відповідає інтересам різних соціальних груп та суспільних інституцій.[2]

Отже, інформаційну політику можна розглядати як діяльність певних суб’єктів, спрямовану на реалізацію та просування власних інтересів у суспільстві через створення, обробку, збереження і поширення різноманітної інформації. Вона виступає важливою сферою суспільного життя, оскільки

---

[1] Коротаєв С. Р. Правові аспекти інформаційного поля України. Національна інформаційна політика. *Актуальні проблеми міжнародних відносин*. Київ, 1997. Вип. 3, ч. 2. С. 58–63.

[2] Васютіна В. В. *Інформаційна політика України в контексті євроінтеграційних процесів* : дис. … канд. політ. наук : 23.00.02. Одеса, 2014. 234 с. URL: http://dspace.pdpu.edu.ua/handle/123456789/327

пов’язана з процесами формування та розповсюдження інформаційних ресурсів, що задовольняють потреби різних соціальних груп і суспільних інституцій.

У стратегічних оцінках НАТО інформаційний вимір прямо пов’язується з гібридними загрозами та використанням дезінформації для впливу на демократичні процеси, підриву суспільної довіри й формування сприятливого середовища для примусу без очевидного переходу до відкритої збройної ескалації.[3]

У цьому контексті інформаційна політика набуває подвійної функції. З одного боку, вона забезпечує легітимацію рішень Альянсу в очах суспільств і партнерів, формує розуміння цілей колективної оборони та кризового реагування. З іншого – вона виконує інструментальну безпекову роль, оскільки стратегічні комунікації (Strategic Communications) розглядаються НАТО як інтегрований підхід до координації різних «інформаційних дисциплін» для підтримки політик, операцій та діяльності Альянсу і досягнення його політичних і військових цілей.[4]

Сьогодні у багатьох зарубіжних державах питання інформаційної політики та інформаційної безпеки посідають важливе місце у державному управлінні та наукових дослідженнях. Починаючи з 1994 року, одним із ключових пріоритетів державної інформаційної політики в різних країнах світу стало формування інформаційного суспільства. Це передбачає підвищення рівня інформаційної культури населення, розвиток інформаційної свідомості громадян, а також активне створення і вдосконалення як національних, так і глобальних інформаційних систем.[5]

Розрізняють державну та недержавну інформаційну політику. Як складова соціальної інформаціології, інформаційна політика має виразний соціально-політичний характер. У цьому контексті її часто пов’язують із

---

[3] NATO 2022 Strategic Concept. Brussels : *NATO, 2022*. URL: https://www.act.nato.int/wp-content/uploads/2023/ 05/290622-strategic-concept.pdf

[4] NATO Strategic Communications Policy. Brussels : *NATO*, [б. р.]. URL: https://info.publicintelligence.net/NATO-STRATCOM-Policy.pdf

[5] Боднар А. О. *Міжнародна інформаційна безпека* : кваліфікаційна робота. Вінниця : Донецький національний університет ім. В. Стуса, 2020. 82 с. URL: https://jarch.donnu.edu.ua/article/view/9490

діяльністю засобів масової інформації, адже саме ЗМІ значною мірою впливають на формування ідеологічних, політичних, економічних та інших суспільних поглядів. Через інформаційні повідомлення, аналітику та інтерпретації вони формують у людей уявлення, знання, оцінки та ставлення до подій, що, у свою чергу, відображається на культурі, поведінці, повсякденному житті й суспільних процесах загалом.[6]

Як наукова категорія інформаційна політика охоплює широку сферу суспільного життя, пов'язану з інформаційними процесами. Її об'єктом є інформаційна сфера суспільства, яка включає інформаційні ресурси, систему інформаційної інфраструктури, різних учасників інформаційної діяльності (тих, хто створює, збирає, обробляє, поширює та використовує інформацію), а також механізми правового й соціального регулювання відносин, що виникають у цих процесах. У межах соціальної інформаціології об'єктом дослідження виступають так звані інформаційні суспільні відносини – взаємодія між суб'єктами, які займаються отриманням, аналізом, поширенням та використанням інформації в інтересах держави і суспільства. З цієї точки зору громадянське суспільство, на яке спрямовується інформаційний вплив, можна розглядати через стан і динаміку суспільної свідомості, що формується під впливом інформаційних процесів.[7]

У загальному вигляді інформаційну політику доцільно розуміти як сукупність цілей, норм, інституційних рішень і практик, за допомогою яких держава або міжнародна організація організовує створення, поширення й захист інформації та вибудовує комунікацію з внутрішніми і зовнішніми аудиторіями задля реалізації політичних та безпекових завдань. Для НАТО це поняття аналітично конкретизується через StratCom: у профільній політиці НАТО стратегічні комунікації визначаються як скоординоване й доречне використання комунікаційних активностей та спроможностей (включно з публічною

---

[6] Васютіна В.В. (2014). *Міжнародна інформаційна* … С. 15.

[7] Васютіна В.В. (2014). *Міжнародна інформаційна* … С. 16.

дипломатією, зв'язками з громадськістю, інформаційними та психологічними операціями) в підтримку політик і діяльності Альянсу.[8]

Теоретичне підґрунтя включення інформаційного виміру до порядку денного міжнародної безпеки пов'язане з «розширенням» поняття безпеки у сучасних дослідженнях та відповідною еволюцією доктрин міжнародних організацій. У стратегічній концепції НАТО 1991 року підкреслено, що безпека і стабільність мають політичні, економічні, соціальні та екологічні складові поряд із незамінним оборонним виміром, а управління різноманіттям викликів потребує широкого підходу до безпеки. У науковій площині близьку логіку розвиває підхід сек'юритизації, пов'язаний із працями Баррі Бузан та Оле Вæвер, де безпека трактується як специфічний тип політики, що може поширюватися на різні суспільні сфери; це дозволяє пояснити, як інформаційні явища набувають статусу безпекових проблем через політичне означення та мобілізацію відповідних інструментів.[9]

Окремий теоретичний пласт формують дослідження публічної дипломатії та «м'якої сили». У класичному підході Джозеф Най комунікація і привабливість цінностей перетворюються на ресурс впливу, здатний доповнювати або частково заміщувати примус. Розгортаючи цю логіку, Джеймс Меліссен описує «нову публічну дипломатію» як мережеву взаємодію з аудиторіями, вбудовану в міжнародну політику, де важливими стають довіра, двосторонність комунікації та здатність інституцій інтерпретувати запити суспільств. Для НАТО ці підходи є методологічно значущими, оскільки інформаційна політика Альянсу об'єктивно працює не лише з державними елітами, а й з масовими аудиторіями, на підтримку яких спирається політична воля до розгортання спроможностей, операцій і партнерських програм.[10]

Аналітичне наповнення інформаційної політики в безпековому вимірі потребує також залучення понять «інформаційне середовище», «інформаційні

---

[8] Васютіна В.В. (2014). *Міжнародна інформаційна* … С. 16.

[9] NATO. The Alliance's New Strategic Concept 1991. Brussels : *NATO*, 1991. URL:https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/1991/11/08/the-alliances-new-strategic-concept-1991

[10] Joseph S. Nye, Jr. (2008). Public Diplomacy and Soft Power. *Public Diplomacy in a Changing World. Vol. 616. pp. 94-109.* https://www.jstor.org/stable/25097996?read-now=1&seq=3

операції» та «інформаційні загрози». У доктринальних документах НАТО інформаційне середовище визначене як поєднання інформації, акторів/систем її передавання та когнітивного, віртуального і фізичного просторів, у яких відбувається сприйняття і циркуляція інформації; технологічний вимір доповнюється тезою, що інформаційні операції (information operations) – це штабна функція планування та інтеграції інформаційних активностей для досягнення бажаних ефектів у свідомості й поведінці цільових аудиторій. Паралельно у тематичних матеріалах НАТО «інформаційні загрози» визначаються як навмисні, шкідливі, маніпулятивні та скоординовані активності державних і недержавних акторів, а дезінформація окреслюється як навмисне поширення хибної або неточної інформації. [11]

Зв'язок інформаційної політики з колективною обороною найвиразніше проявляється через феномен гібридних загроз. НАТО розглядає гібридні загрози як комплексне використання як військових, так і невійськових інструментів – як відкритих, так і прихованих засобів. До них належать, зокрема, дезінформаця та кібератаки, мета яких – стерти межу між станом війни та миру і підрвати стабільність суспільства; водночас підкреслюється пріоритет підготовки, стримування і захисту від таких впливів. В академічній літературі співзвучний аналіз пропонує Френк Гоффман, який окреслює гібридну війну як поєднання різнорідних способів застосування сили і впливу, включно з експлуатацією інформаційного домену. Поєднання цих підходів дає змогу розглядати інформаційну політику НАТО як інструмент підвищення стійкості до гібридних дій та як механізм підтримки колективної оборони в ситуаціях, де «поріг» збройного нападу навмисно розмивається. [12]

Місце інформаційної політики в системі міжнародної безпеки проявляється також у діяльності міжнародних організацій, що формують нормативні рамки для інформаційної безпеки та протидії деструктивним

---

[11] UK Ministry of Defence. AJP-10 Allied Joint Doctrine for Strategic Communications. Change 1. London : *UK MoD*, 2023. URL: https://assets.publishing.service.gov.uk/media/6525459d244f8e00138e7343/AJP_10_Strat_Comm_Change_1_web.pdf

[12] NATO. Countering Hybrid Threats. Brussels : *NATO*, [б. р.]. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

впливам. На глобальному рівні питання міжнародної інформаційної безпеки та використання ІКТ у контексті міжнародної безпеки закріплюються у резолюціях Організації Об'єднаних Націй. На регіональному рівні Організація з безпеки і співробітництва в Європі ухвалювала початковий набір заходів зміцнення довіри для зниження ризиків конфлікту, пов’язаних із використанням ІКТ. У межах Європейський Союз протидія дезінформації була оформлена у вигляді спеціального плану дій, спрямованого на підвищення спроможності виявляти та нейтралізувати дезінформаційні впливи та зміцнювати суспільну стійкість. Таким чином, інформаційна політика НАТО функціонує не у вакуумі, а в ширшій архітектурі міжнародної безпеки, де різні організації взаємодіють через норми, координацію та обмін практиками. [13]

Таким чином, інформаційна політика виведена за межі «публічних комунікацій» у вузькому сенсі й інтерпретується як інтегрований напрям міжнародної безпеки, де поєднуються стратегічні комунікації (Strategic Communications), інформаційна безпека, протидія дезінформації та управління інформаційним середовищем, включно з протидією інформаційним операціям у межах гібридних загроз. Для НАТО це означає поєднання вимірів легітимації, стійкості та інструментальної підтримки політичних і військових цілей, що знаходить відображення як у доктринальному визначенні інформаційних загроз, так і в стратегічних оцінках сучасного безпекового середовища.

1.2. Понятійно-категоріальний апарат та методи дослідження

У витоках комунікаційної складової Альянсу простежується логіка забезпечення суспільної підтримки колективної оборони в умовах ідеологічної конфронтації: дослідження з історії публічної дипломатії НАТО вказують, що 1950 року Північноатлантична рада визначила завдання координації публічної інформації, а впродовж першої половини 1950-х було інституційно оформлено інформаційну службу і суміжні механізми комунікації політик Альянсу. Водночас у цій літературі підкреслюється, що в період Холодної війни

[13] United Nations General Assembly. Resolution 78/237. New York : *UN*, 2023. URL: https://docs.un.org/en/a/res/78/237

комунікаційна діяльність НАТО розвивалася у тіні ширшого ідеологічного протистояння та була обмежена рамками сприйняття Альянсу як насамперед військово-політичного блоку. [14]

Після завершення Холодної війни стратегічні концепти НАТО 1991 і 1999 років закріпили зсув до ширшого безпекового порядку денного, де поряд із колективною обороною зростає значення кризового менеджменту, партнерств і політичної координації. Для інформаційної політики це означало перехід від відносно «сталої» логіки стримування до завдання пояснення багатовимірної ролі Альянсу і формування суспільної підтримки для нових форматів діяльності.[15]

Інституційним відображенням трансформації стало посилення публічної дипломатії й створення у 2003 році профільного підрозділу НАТО в Брюссель. У дослідженні Стефані Бабст наголошується, що цей підрозділ виник як відповідь на потребу модернізувати комунікацію Альянсу та краще пояснювати місію НАТО для нових поколінь і політичних еліт; у тому ж контексті підкреслюється роль тодішнього генерального секретаря Джорджа Робертсона у створенні цієї структури. Відповідно «інформаційна політика» поступово набуває інституційної форми, яка дозволяє Альянсу системно працювати з легітимністю та суспільним сприйняттям у новому безпековому середовищі.[16]

Подальша еволюція стратегічної рамки відображена у саміті в Ризі (2006), де у Ризькій декларації зафіксовано схвалення «Комплексних політичних настанов» як рамки та політичного спрямування для продовження трансформації НАТО на горизонті 10–15 років. «Комплексні політичні настанови» задають логіку узгодження пріоритетів та інструментів планування,

---

[14] Güleç C. NATO and Public Diplomacy: Opportunities and Constraints of 21st Century. *Perceptions*. 2021. Vol. XXVI, № 1. P. 100–120. URL: https://dergipark.org.tr/tr/download/article-file/1905361

[15] NATO. The Alliance's New Strategic Concept 1991. Brussels : *NATO*, 1991. URL: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/1991/11/08/the-alliances-new-strategic-concept-1991

[16] Babst, St. Reinventing NATO's public diplomacy. *Research Paper.* №41. 8 p., 2008. URL: https://www.files.ethz.ch/isn/94347/rp_41en.pdf

що підвищує вимоги до узгодженої комунікації Альянсу в умовах розширення партнерств і спектра місій.[17]

Нормативно-доктринальна інституціоналізація стратегічних комунікацій чітко простежується з кінця 2000-х. У комюніке НАТО 2008 року наголошено, що сучасне інформаційне середовище потребує належної, своєчасної, точної та чутливої комунікації з локальними й міжнародними аудиторіями щодо політик та участі в міжнародних операціях. Наступного року у декларації саміту, що відбувся у Страсбурзі та Кель, підкреслено, що стратегічні комунікації є невід'ємною частиною зусиль Альянсу з досягнення політичних і військових цілей.[18]

Ключовим кроком стала «NATO Strategic Communications Policy» (2009), яка закріплює інтегрувальне визначення StratCom як скоординованого використання публічної дипломатії, цивільних і військових зв'язків із громадськістю, інформаційних операцій та психологічних операцій. У документі визначено принципи, релевантні для інформаційної політики Альянсу: послідовність повідомлень на всіх рівнях, активна присутність в інформаційному середовищі зі швидким реагуванням, вимоги точності й ясності, орієнтація на вимірювання ефективності та широке охоплення комунікаційних каналів, включно із механізмами отримання зворотного зв'язку.[19]

Військово-доктринальний вимір підкреслює підпорядкованість інформаційної політики політичному керівництву та уточнює роль інформаційних операцій у межах StratCom. Доктрина AJP-3.10 наголошує на цивільно-політичній першості в інформаційних питаннях і описує Info Ops як інструмент військового компонента, що має інтегруватися у планування й реалізацію операцій з урахуванням політичної чутливості та участі

---

[17] NATO. Riga Summit Declaration. Brussels : *NATO*, 2006. URL: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2006/11/29/riga-summit-declaration

[18] NATO. Bucharest Summit Declaration. Brussels : *NATO*, 2008. URL: https://www.nato.int/cps/en/natolive/official_texts_46247.htm

[19] NATO. NATO Strategic Communications Policy. Brussels : *NATO*, [б. р.]. URL: https://info.publicintelligence.net/NATO-STRATCOM-Policy.pdf

невійськових акторів. Доктрина AJP-10, зі свого боку, демонструє вбудованість військової політики зі стратегічних комунікацій у ширшу ієрархію документів НАТО, що засвідчує інституційну зрілість StratCom як механізму, який поєднує політичні настанови та операційну практику.[20]

Важливим рубежем постхолодновоєнної еволюції стала Стратегічна концепція НАТО 2010 року, ухвалена на саміті у Лісабоні. Документ підкреслює необхідність тіснішої співпраці з міжнародними партнерами, насамперед з ООН та ЄС, і фіксує розвиток здатності протидії кібератакам як один із напрямів спроможнісного розвитку. У цьому контексті інформаційна політика набуває ролі «з'єднувальної тканини» між політичними рішеннями, операційним плануванням і партнерською взаємодією.[21]

Після 2014 року еволюція інформаційної політики НАТО дедалі тісніше пов'язується з протидією гібридним загрозам і дезінформації, що стало помітним на тлі російської агресії проти Україна. У декларації саміту в Уельсі (2014) НАТО включає до реагування на гібридні загрози підсилення стратегічних комунікацій і вітає створення Центру передового досвіду НАТО зі стратегічних комунікацій у Латвії; у зовнішніх аналітичних оглядах також підкреслено, що операційний досвід (зокрема у Афганістані) та виклики «битви наративів» стали важливими факторами посилення StratCom у НАТО.[22]

На саміті у Варшаві (2016) ця логіка була конкретизована політичними рішеннями: у Варшавському комюніке гібридну війну описано як комплексне поєднання конвенційних і неконвенційних, відкритих і прихованих засобів, а також зафіксовано ухвалення стратегії та планів імплементації ролі НАТО в протидії гібридній війні з наголосом на координації з ЄС. Комюніке також

---

[20] NATO. AJP-3.10 Allied Joint Doctrine for Information Operations. Ed. A, Ver. 1. Brussels : *NATO*, 2019. URL: https://mpsotc.army.gr/wp-content/uploads/2024/03/2.-AJP-3.10-EDA-V1-E.pdf

[21] NATO. Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of NATO. Brussels : *NATO*, 2010. URL: https://www.nato.int/content/dam/nato/legacy-wcm/media_pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

[22] NATO. Wales Summit Declaration : Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales, 05 September 2014. Brussels : *NATO*, 2014. URL:https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2014/09/05/wales-summit-declaration

підкреслює, що НАТО готове допомагати союзнику на будь-якому етапі гібридної кампанії, а в політичному вимірі Альянс розглядає можливість застосування колективної оборони у разі ескалації гібридних дій до рівня, порівнюваного зі збройним нападом; водночас у комюніке фіксується намір удосконалювати стратегічні комунікації як частину інституційної адаптації.[23]

Таким чином, еволюція інформаційної політики НАТО простежується як перехід від ранніх інформаційних інструментів епохи Холодної війни до інституційно оформленої системи стратегічних комунікацій, інтегрованої в політичне та операційне планування й орієнтованої на протидію гібридним загрозам. Сучасні принципи цієї політики можна узагальнити як поєднання «єдності повідомлень» і узгодженості слів із діями; швидкості, точності й ясності комунікації в реальному інформаційному циклі; вимірюваності ефектів та широкого охоплення каналів; а також інституційної координації між цивільними і військовими елементами в межах політичного керівництва Альянсу.

Подальший розвиток інформаційної політики НАТО пов’язаний із посиленням ролі інформаційного середовища як самостійного простору стратегічної взаємодії. Одним із ключових інституційних елементів розвитку стратегічних комунікацій стало створення та діяльність Центру передового досвіду НАТО зі стратегічних комунікацій у Ризі. Центр був заснований у 2014 році з метою розвитку комунікаційних спроможностей Альянсу, проведення досліджень інформаційного середовища, аналізу інформаційних операцій та підготовки експертів у сфері стратегічних комунікацій. Його діяльність спрямована на надання аналітичної підтримки державам-членам НАТО, розроблення концепцій та практичних рекомендацій щодо протидії інформаційним загрозам, а також розвиток освітніх і тренінгових програм у сфері StratCom.[24]

---

[23] NATO. Warsaw Summit Communiqué. Brussels : *NATO*, 2016. URL: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique

[24] NATO ACT. StratCom COE 2024. *ACT NATO*. 2024. URL: https://www.act.nato.int/article/stratcom-coe-2024/

Важливим напрямом роботи Центру є дослідження нових форм інформаційного впливу, зокрема використання цифрових технологій, соціальних мереж та штучного інтелекту для поширення маніпулятивних наративів. У зв'язку з цим стратегічні комунікації НАТО дедалі більше орієнтуються на аналіз цифрового інформаційного середовища, розроблення механізмів раннього виявлення інформаційних операцій та формування стійкості суспільства до інформаційного впливу.[25]

На сучасному етапі інформаційна політика НАТО спирається на низку базових принципів, що визначають характер комунікаційної діяльності Альянсу. Передусім йдеться про принцип достовірності та прозорості комунікації. У демократичних політичних системах збереження довіри громадян є критично важливим, тому інформаційна політика НАТО базується на необхідності надання правдивої, перевіреної та зрозумілої інформації щодо діяльності Альянсу. Саме довіра та авторитет комунікації розглядаються як основа ефективності стратегічних повідомлень і запорука суспільної підтримки колективної безпеки.[26]

Важливою характеристикою сучасної інформаційної політики НАТО є також її проактивний характер. Якщо на ранніх етапах діяльності Альянсу комунікаційна політика часто мала реактивний характер і була спрямована на пояснення вже прийнятих рішень, то сьогодні комунікація розглядається як інструмент формування стратегічного середовища. Це означає активну участь НАТО в інформаційному просторі, своєчасне донесення позиції Альянсу та формування позитивного наративу щодо його ролі у забезпеченні міжнародної безпеки.

Особливе місце в інформаційній політиці Альянсу займає принцип інституційної координації. Стратегічні комунікації об'єднують різні комунікаційні інструменти – публічну дипломатію, зв'язки із засобами масової інформації, інформаційні операції та інші форми комунікаційної діяльності.

---

[25] NATO ACT. NATO StratCom COE. *ACT NATO*. [б. р.]. URL: https://www.act.nato.int/article/nato-stratcom-coe/

[26] Joint Air Power Competence Centre. C-UAS Strategic Communications. *JAPCC*. [б. р.]. URL: https://www. japcc.org/chapters/c-uas-strategic-communications/

Координація цих інструментів дозволяє забезпечити системний вплив на інформаційне середовище та підвищити ефективність комунікаційних стратегій НАТО.[27]

Таким чином, сучасний етап розвитку інформаційної політики НАТО характеризується поглибленням інтеграції стратегічних комунікацій у систему безпекової політики Альянсу. Інформаційний вимір дедалі більше розглядається як один із ключових елементів стратегічної конкуренції у міжнародному середовищі. У цих умовах інформаційна політика НАТО поєднує традиційні принципи демократичної комунікації – відкритість, достовірність і підзвітність – із новими інструментами протидії інформаційним загрозам та гібридним формам впливу.

Висновки до Розділу 1

У першому розділі встановлено, що інформаційна політика в сучасній системі міжнародної безпеки є важливим інструментом реалізації політичних і безпекових цілей. Вона охоплює не лише створення та поширення інформації, а й захист інформаційного простору, підтримку легітимності рішень і протидію деструктивним інформаційним впливам. З'ясовано, що в діяльності НАТО інформаційна політика реалізується через систему стратегічних комунікацій, які забезпечують скоординоване використання комунікаційних інструментів на підтримку політики та операцій Альянсу. Інформаційний вимір виконує подвійну функцію: пояснення рішень НАТО суспільствам і партнерам та підвищення стійкості до інформаційних впливів у межах колективної оборони. Аналіз еволюції інформаційної політики НАТО показав її трансформацію від моделі публічного інформування часів Холодної війни до інституційно сформованої системи стратегічних комунікацій, інтегрованої в політичне та безпекове планування. Встановлено, що сучасна інформаційна політика Альянсу базується на принципах достовірності, прозорості, послідовності,

[27] Strategic Communication: A Caution to Military Commanders. *Military Review.* 2017. November. URL: https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2017-Online-Exclusive-Articles/Strategic-Communication/

проактивності та міжінституційної координації, а також орієнтації на вимірювання ефективності комунікацій і підвищення суспільної стійкості до інформаційних загроз. Таким чином, інформаційна політика НАТО є складним багаторівневим явищем, що поєднує політичні, комунікаційні та безпекові інструменти і виступає важливою складовою системи колективної оборони та протидії гібридним загрозам.

РОЗДІЛ 2
СУЧАСНІ ЗАГРОЗИ ТА ВИКЛИКИ ІНФОРМАЦІЙНІЙ ПОЛІТИЦІ НАТО

2.1. Інформаційні та гібридні загрози в умовах сучасних конфліктів

Розвиток інформаційного суспільства та цифрових технологій істотно змінив характер конфліктів і конкуренції між державами: поряд із традиційними військовими засобами дедалі активніше застосовуються інструменти впливу на інформаційне середовище, здатні підривати довіру, поляризувати суспільства та послаблювати спроможність держав ухвалювати рішення. У Стратегічній концепції НАТО 2022 року наголошено, що стратегічні конкуренти випробовують стійкість демократичних суспільств, застосовують гібридні тактики та використовують дезінформацію і маніпуляцію як засоби тиску, підриву й дестабілізації.[28]

У документах НАТО останніх років простежується інституціоналізація цієї проблематики: підхід Альянсу до протидії інформаційним загрозам (2024) визначає їх як умисні, шкідливі та скоординовані дії в інформаційному середовищі, включно з інформаційними операціями (Information Operations) та дезінформацією (Disinformation), і орієнтує держави-члени на системні відповіді, сумісні з демократичними стандартами та цінностями.[29]

Ключовим є розкриття понять «гібридні загрози» та «інформаційні загрози» як категорій, що пояснюють сучасну трансформацію військово-політичного протистояння. НАТО визначає гібридні загрози як поєднання військових і невійськових, прихованих і відкритих засобів, серед яких прямо називаються дезінформацією, кібератаки, економічний тиск та інші інструменти, покликані «розмивати» межі між війною і миром та

---

[28] NATO. NATO 2022 Strategic Concept. Brussels : *NATO*, 2022. URL: https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept-ukr.pdf

[29] NATO's Approach to Counter Information Threats : Official text, 18 October 2024. *NATO*. URL: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/10/18/natos-approach-to-counter-information-threats

дестабілізувати суспільства.[30] У такій логіці Hybrid Warfare постає не як «альтернатива» класичній війні, а як спосіб досягнення стратегічних цілей через комбінування інструментів примусу і впливу, де інформаційний компонент є системоутворювальним елементом.

Роль інформаційного виміру в сучасних конфліктах проявляється в тому, що боротьба за інтерпретацію подій і легітимність дій нерідко стає «паралельним фронтом», який впливає на мобілізацію ресурсів, підтримку союзників і стійкість суспільств. НАТО у своїх публічних поясненнях щодо протидії дезінформації наголошує, що сучасні кампанії можуть «сіяти розбрат» і підривати демократії та здатність діяти, а відповідь має включати аналіз інформаційного середовища, проактивну комунікацію та викриття ключових випадків дезінформації.[31]

Трансформація конфліктів у цифрову епоху полягає не лише в появі нових платформ комунікації, а й у структурній зміні швидкості та масштабу поширення впливів. НАТО підкреслює, що новим у сучасних гібридних атаках є їхня швидкість, масштаб і інтенсивність, посилені технологічними змінами та глобальною взаємопов'язаністю.[32] Водночас Стратегічна концепція 2010 року, сформульована на тлі швидкої цифровізації, зафіксувала, що кібератаки здатні досягати порогу, який загрожує безпеці й стабільності, тобто вимагають включення цифрових ризиків до порядку денного колективної оборони.[33] У практичному вимірі це означає, що інформаційні операції історично «вбудувалися» у цифрову інфраструктуру: від бот-мереж та координованої неавтентичної поведінки до «hack-and-leak» і підміни джерел, що ускладнює відмежування інформаційного впливу від кібердій.

---

[30] Countering Hybrid Threats. Updated: 29 January 2026. *NATO*. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

[31] How Does NATO Respond to Disinformation? *NATO News*. 25 May 2021. *NATO*. URL: https://www.nato.int/en/news-and-events/articles/news/2021/05/25/how-does-nato-respond-to-disinformation

[32] Countering Hybrid Threats. Updated: 29 January 2026. *NATO*. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

[33] NATO. Bucharest Summit Declaration. Brussels : *NATO*, 2008. URL: https://www.nato.int/cps/en/natolive/official_texts_46247.htm

У цьому контексті особливого значення набуває доктрина стратегічних комунікацій (Strategic Communications) як спосіб синхронізувати політичні рішення, воєнні дії та комунікаційний супровід. Політика Strategic Communications 2009 року виходить з того, що сучасне медійне середовище та інтенсивний інформаційний цикл безпосередньо впливають на сприйняття операцій і політик НАТО, а отже – на їхню результативність і легітимність. Тому Public Diplomacy, Public Affairs, Information Operations та Psychological Operations мають застосовуватися скоординовано й «належним» чином, щоб мінімізувати суперечності, які можуть бути експлуатовані опонентом у межах Hybrid Warfare.[34]

Емпірична логіка інформаційних операцій у військово-політичному протистоянні особливо виразна у російсько-українській війні, де одночасно застосовуються військова сила, кіберактивність і систематичний інформаційний тиск. Показовим прикладом поєднання кібер та інформаційного виміру стала атака на супутникову мережу KA-SAT компанії Viasat у день початку широкомасштабного вторгнення: у заяві від імені Європейський Союз (ЄС) зазначено, що кібератака відбулася за годину до вторгнення, «полегшивши» військову агресію, та спричинила невибіркові перебої зв'язку й порушення комунікацій для органів влади, бізнесу і користувачів в Україні, а також у низці держав-членів ЄС.[35] У безпековому сенсі такі інциденти мають подвійний ефект: вони підривають інфраструктурну стабільність і водночас продукують інформаційний сигнал про вразливість та «контроль» над середовищем.

Додатковим прикладом є кампанія NotPetya 2017 року, яку Велика Британія публічно атрибутувала російському державному актору, підкресливши

---

[34] NATO. NATO Strategic Communications Policy. Brussels : *NATO*, [б. р.]. URL: https://info.publicintelligence.net/NATO-STRATCOM-Policy.pdf

[35] Russian Cyber Operations Against Ukraine : Declaration by the High Representative on Behalf of the European Union, 10 May 2022. *Council of the European Union.* URL: https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

руйнівну мету та невибірковий дизайн, що спричинив поширення за межі первинної зони ураження й значні економічні наслідки в Європі.[36]

Подальший розвиток інформаційних і гібридних загроз пов'язаний із появою нових форм впливу на суспільства, які виходять за межі традиційної пропаганди або інформаційних операцій. У сучасних дослідженнях дедалі частіше використовується поняття когнітивного виміру конфлікту, що передбачає цілеспрямований вплив на процеси мислення, інтерпретації інформації та ухвалення рішень у суспільстві. У межах цієї логіки інформаційні кампанії спрямовані не лише на зміну конкретних поглядів, а й на формування нових способів сприйняття реальності, що здатні впливати на поведінку індивідів, соціальних груп і політичних інститутів.[37]

Когнітивний вимір інформаційного протистояння особливо актуалізувався у зв'язку з розвитком цифрових платформ та алгоритмічних систем поширення інформації. Соціальні мережі, пошукові алгоритми та системи персоналізованих рекомендацій створюють умови для швидкого масштабування інформаційних впливів і точкового таргетування окремих аудиторій. У таких умовах дезінформаційні кампанії можуть поєднувати традиційні пропагандистські методи з автоматизованими технологіями поширення контенту, включно з використанням бот-мереж, фейкових акаунтів і координованої неавтентичної поведінки. Подібні кампанії часто мають на меті посилення поляризації суспільства, підрив довіри до інституцій або дискредитацію політичних рішень.[38]

У контексті гібридних конфліктів такі інструменти використовуються у поєднанні з іншими формами тиску – політичним, економічним або військовим. Саме комбінування різнорідних інструментів і становить сутність гібридної війни, яка поєднує військові та невійськові, відкриті та приховані засоби впливу,

---

[36] Foreign Office Minister Condemns Russia for NotPetya Attacks. *UK Foreign & Commonwealth Office*. URL: https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks

[37] Cognitive Warfare. *NATO ACT*. URL: https://www.act.nato.int/activities/cognitive-warfare/.

[38] Strategic communication and countering foreign information manipulation and interference. *European Commission*. URL: https://commission.europa.eu/topics/countering-information-manipulation_en

включно з дезінформацією, кібератаками та економічним тиском. Основною метою таких дій є створення ситуації невизначеності та підрив довіри в суспільстві, що ускладнює ефективну реакцію держав і міжнародних організацій.[39]

Окремим елементом сучасних гібридних загроз є активне використання кіберпростору як інструменту стратегічного впливу. Кібероперації здатні виконувати не лише технічні або інфраструктурні функції, а й комунікаційні – демонструвати вразливість державних систем, формувати атмосферу невизначеності та підривати довіру до державних інституцій. У документах НАТО підкреслюється, що кіберзагрози є дедалі більш складними, руйнівними та частими, а кіберпростір постійно перебуває у стані конкуренції між державними і недержавними акторами.[40]

Зростання ролі інформаційного виміру конфліктів також пов’язане з розширенням кола акторів, здатних здійснювати інформаційний вплив. Якщо раніше ключову роль у таких операціях відігравали державні структури, то сьогодні до них можуть долучатися недержавні організації, приватні компанії, медіаплатформи та навіть окремі користувачі цифрових мереж. Така децентралізація інформаційного середовища ускладнює процес атрибуції інформаційних атак і створює додаткові виклики для міжнародної безпеки.

Дедалі більшого значення набуває міжнародна координація у сфері протидії гібридним загрозам. НАТО та Європейський Союз розвивають спільні механізми аналізу інформаційних впливів, обміну даними та координації стратегічних комунікацій, що дозволяє більш ефективно реагувати на транскордонні інформаційні кампанії. Така взаємодія є важливою з огляду на те, що сучасні інформаційні операції часто спрямовані одночасно на кілька держав або регіонів.

Таким чином, інформаційні та гібридні загрози в умовах сучасних конфліктів формують складну систему взаємопов’язаних впливів, у межах якої

---

[39]Countering Hybrid Threats. Updated: 29 January 2026. *NATO*. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

[40]Cyber Defence. *NATO*. URL:https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence

інформаційні операції, кіберактивність і психологічні методи впливу функціонують як елементи єдиної стратегії. У цифрову епоху інформаційний простір перетворюється на ключове поле стратегічної конкуренції, де боротьба за інтерпретацію подій, довіру громадян і легітимність політичних рішень набуває не меншого значення, ніж традиційні військові інструменти. Саме тому для НАТО та його союзників управління інформаційним середовищем, розвиток стратегічних комунікацій і підвищення стійкості суспільств розглядаються як необхідні складові сучасної системи безпеки.

2.2. Дезінформація, пропаганда та інформаційні операції як інструменти впливу

Зосередимось на аналізі дезінформації, пропаганди та Information Operations як інструментів впливу на суспільство, політику та міжнародну безпеку. У публічних матеріалах НАТО підкреслюється, що дезінформація не є новим явищем, однак сучасний інформаційний ландшафт радикально збільшив її масштаб і складність, зробивши «озброєння інформації» доступнішим і значно більш керованим у часі.[41] Подібну логіку фіксує і політичний документ Організація Об’єднаних Націй (ООН) щодо information integrity: цифрові платформи, одночасно підсилюючи зв’язність і доступ до інформації, створили умови для швидкого поширення брехні та ненависті, що може мати «реальну шкоду» для миру, демократії та прав людини.[42]

Водночас сучасне інформаційне середовище характеризується не лише швидкістю поширення контенту, але й високим рівнем його технологічної обробки. Алгоритми соціальних мереж, системи персоналізованих рекомендацій та інструменти мікротаргетингу дозволяють адресно впливати на конкретні соціальні групи або навіть окремих користувачів. У результаті

---

[41] How Does NATO Respond to Disinformation? *NATO News*. 25 May 2021. *NATO*. URL: https://www.nato.int/en/news-and-events/articles/news/2021/05/25/how-does-nato-respond-to-disinformation

[42] United Nations. Our Common Agenda : Policy Brief — Information Integrity on Digital Platforms. New York : *UN*, 2023. URL: https://brasil.un.org/sites/default/files/2023-06/our-common-agenda-policy-brief-information-integrity-en.pdf

дезінформаційні повідомлення можуть бути адаптовані до психологічних характеристик аудиторії, її політичних переконань або інформаційних уподобань, що значно підвищує ефективність маніпулятивних кампаній. Саме тому сучасні дослідники дедалі частіше говорять про перехід від традиційної пропаганди до більш складних форм інформаційного впливу, які поєднують комунікаційні, технологічні та психологічні інструменти.

У науковій літературі сучасні інформаційні кампанії дедалі частіше розглядаються як складова ширшого феномену інформаційної війни. У межах цього підходу поширення пропаганди та дезінформації розглядається як спосіб маніпуляції інформаційним середовищем з метою деморалізації опонента, формування вигідних наративів і підриву довіри до державних інституцій. Інформаційна війна може включати збір і контроль інформації, поширення пропагандистських повідомлень та обмеження доступу супротивника до достовірних джерел, що робить її важливим інструментом стратегічного протистояння між державами.[43]

Поняттєве розмежування є принциповим: у підході ООН дезінформація пов’язується з умислом вводити в оману та завдавати шкоди, тоді як misinformation описує неумисне поширення неточної інформації «в добрій вірі».[44] Для НАТО це розрізнення має практичну цінність, оскільки дозволяє відокремлювати захист інформаційного середовища від криміналізації помилок або критики й фокусуватися на умисних, скоординованих операціях, що кваліфікуються як інформаційні загрози та hostile information activities.[45]

Важливість такого розмежування полягає також у тому, що воно визначає характер політичної та правової відповіді на інформаційні загрози. Якщо

---

[43] Letzing J. What Is Information Warfare and How Pervasive Is It? *World Economic Forum*. 14 April 2022. URL: https://www.weforum.org/stories/2022/04/what-is-information-warfare-and-how-pervasive-is-it/

[44] United Nations. Our Common Agenda : Policy Brief — Information Integrity on Digital Platforms. New York : *UN*, 2023. URL: https://brasil.un.org/sites/default/files/2023-06/our-common-agenda-policy-brief-information-integrity-en.pdf

[45] NATO's Approach to Counter Information Threats : Official text, 18 October 2024. *NATO*. URL: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/10/18/natos-approach-to-counter-information-threats

misinformation переважно пов’язана з проблемами інформаційної грамотності або недостатньої перевірки фактів, то дезінформація розглядається як навмисна діяльність, яка може бути організована державними або недержавними акторами з метою досягнення конкретних політичних результатів. Саме тому протидія дезінформації передбачає не лише розвиток медіаграмотності, а й створення механізмів аналітики інформаційного середовища, виявлення координованих інформаційних кампаній та зміцнення міжнародної співпраці у сфері інформаційної безпеки.

Механізми впливу дезінформації та пропаганди ґрунтуються на поєднанні когнітивних, емоційних і соціальних чинників: маніпуляція працює через селекцію фактів, повторюваність, апеляцію до страху або образу, створення уявлення про «консенсус» та ерозію довіри до офіційних джерел. НАТО прямо зазначає, що ворожі наративи та пропаганда можуть комбінуватися з дезінформацією для сіяння розбрату і підриву демократичних інституцій та здатності діяти, тобто мають чітко виражену безпекову функцію.[46] У межах сучасних конфліктів це означає, що інформаційні операції впливають не лише на «думку», а й на практичну поведінку: від готовності до колективних дій до підтримки рішень про санкції, допомогу союзникам чи реформування оборонних політик.

У сучасних інформаційних кампаніях важливу роль відіграє так званий «наративний дизайн». Він передбачає створення повторюваних сюжетних ліній, які формують альтернативну картину реальності. Такі наративи можуть включати історичні міфи, теорії змови або емоційно забарвлені повідомлення, що апелюють до страху, несправедливості чи образи. Дослідження НАТО підкреслюють, що подібні кампанії здатні маніпулювати громадською думкою, поляризувати суспільства та підривати внутрішню згуртованість держав.[47]

---

[46] How Does NATO Respond to Disinformation? *NATO News*. 25 May 2021. *NATO*. URL: https://www.nato.int/en/news-and-events/articles/news/2021/05/25/how-does-nato-respond-to-disinformation

[47] The Cognitive Battlefield of Hybrid Warfare. *NATO Defense College Foundation.* URL: https://www.natofoundation.org/food/the-cognitive-battlefield-of-hybrid-warfare/

У сучасному інформаційному просторі особливої ваги набуває питання акторності: поряд із державними суб'єктами активно діють недержавні мережі, комерційні «постачальники маніпуляцій», інфлюенсери, а також технічні посередники – цифрові платформи.

Дослідження NATO Strategic Communications Centre of Excellence щодо соціальної маніпуляції (експеримент 2022/2023) демонструє, що зусилля платформ у протидії комерційній маніпуляції загалом стагнують, а значна частка неавтентичної взаємодії зберігається протягом тривалого часу. Важливим є і якісне наповнення цього феномену: маніпулятивні практики включають бот-кероване підсилення, використання фейкових акаунтів, «hack-and-leak» операції, імітацію осіб та поширення malicious deepfakes. Згідно з висновками звіту, переважна частка придбаної неавтентичної взаємодії залишалася активною через чотири тижні після повідомлення про неї, а доставка маніпулятивної взаємодії в більшості випадків ставала майже миттєвою, що створює асиметрію на користь маніпуляторів.[48]

Політичний документ ООН застерігає, що дискурс «боротьби з дезінформацією» може використовуватися окремими державами як привід для надмірних обмежень доступу до інформації та тиску на журналістів і опонентів, а тому відповіді мають бути правовими, пропорційними та прозорими.[49]

Альянс змушений поєднувати стійкість до інформаційних маніпуляцій із демонстрацією ціннісної відмінності від авторитарних практик і збереженням довіри до демократичних інститутів як «центру тяжіння» колективної безпеки.

Як приклад інформаційних кампаній, спрямованих на демократичні суспільства, можна розглянути стійкі наративи щодо ролі НАТО у війні та причин конфлікту, які Альянс системно спростовує. У матеріалах «Setting the

---

[48] Fredheim R., Bay S., Haiduchyk T., Dek A., Stolze M. Social Media Manipulation 2022/2023 : Assessing the Ability of Social Media Companies to Combat Platform Manipulation. Riga : *NATO StratCom COE*, 2023. URL: https://stratcomcoe.org/publications/download/Social-Media-Manipulation-2022-2023-DIGITAL.pdf

[49] United Nations. Our Common Agenda : Policy Brief — Information Integrity on Digital Platforms. New York : *UN*, 2023. URL: https://brasil.un.org/sites/default/files/2023-06/our-common-agenda-policy-brief-information-integrity-en.pdf

record straight» зазначено, що Росія використовує звичайні, кібернетичні та гібридні засоби, включно з дезінформацією, проти союзників і партнерів, а також наведено характерні міфи, наприклад твердження, що «НАТО воює з Росією в Україні» або що Альянс «пообіцяв не розширюватися» після Холодної війни; їхня функція в такому контексті полягає в делегітимації західної коаліційної взаємодії та ерозії підтримки України.[50] Для інформаційної політики НАТО ці приклади важливі тим, що демонструють сталість і «репродукованість» дискурсивних шаблонів, які активуються під час ескалацій, а отже потребують не лише реактивного спростування, а і довгострокових механізмів підвищення стійкості аудиторій.

У контексті російсько-української війни інформаційні операції стали важливим інструментом геополітичного впливу. Державні медіа та пов'язані з ними мережі поширювали повідомлення, що заперечують українську державність, звинувачують Україну у вигаданих злочинах або стверджують, що НАТО контролює українську політику. Подібні наративи спрямовані на підрив міжнародної підтримки України та формування сумнівів у легітимності її боротьби за суверенітет.[51]

Виклик для інформаційної політики НАТО полягає в тому, що дезінформація, пропаганда та інформаційні операції діють на стику між свободою публічної сфери і безпековою вразливістю відкритих демократичних систем. Саме тому НАТО наголошує, що відповідь має базуватися на прозорості, аналізі інформаційного середовища, проактивній комунікації та викритті ключових випадків дезінформації, а також на співпраці з партнерами, оскільки «діяти самостійно» недостатньо. У рамках Strategic Communications це означає поєднання інформаційних заходів із політико-військовими

---

[50]Setting the Record Straight. *NATO*. URL: https://www.nato.int/en/what-we-do/wider-activities/natos-approach-to-counter-information-threats/setting-the-record-straight

[51] War Speeches, Negotiations, War with NATO and the Absence of Ukraine: What Did Russia Lie About in January? *Opora Ukraine*. URL: https://oporaua.org/en/viyna/war-speeches-negotiations-war-with-nato-and-the-absence-of-ukraine-what-did-russia-lie-about-in-january-25092

рішеннями таким чином, щоб слова, дії та інституційні практики були взаємно підкріплювальними, а не суперечливими.[52]

У стратегічному вимірі ці інструменти дедалі частіше розглядаються як складова ширшої концепції гібридного протистояння. Дезінформація, пропаганда та інформаційні операції можуть використовуватися паралельно з кібератаками, економічним тиском або дипломатичними маніпуляціями. Саме поєднання різнорідних інструментів створює ефект «гібридного тиску», у межах якого інформаційний вплив стає ключовим механізмом формування сприятливого стратегічного середовища для досягнення політичних і військових цілей.

Таким чином, можна стверджувати, що дезінформація, пропаганда та інформаційні операції становлять виклик для НАТО не лише як «інформаційні інциденти», а як системні інструменти впливу, здатні підривати легітимність, згуртованість і стійкість демократичних суспільств. У цифрову епоху особливо зростає роль платформної архітектури та комерціалізації маніпуляцій, що вимагає від інформаційної політики НАТО поєднання фактологічної проактивності, аналітики інформаційного середовища та узгодженої взаємодії з партнерами для мінімізації гібридних ефектів.

2.3. Вплив зовнішніх і внутрішніх чинників на інформаційну стійкість НАТО

Сучасна архітектура безпеки Північноатлантичного альянсу зазнає фундаментальної трансформації, де інформаційна стійкість (information resilience) перетворюється з допоміжного елемента на критично важливу складову колективної оборони. Стратегічна концепція НАТО 2022 року чітко визначає, що стійкість є центральним чинником виконання трьох основних завдань Альянсу: стримування та оборони, запобігання кризам та управління ними, а також безпеки на основі співробітництва. [1] В умовах, коли межа між миром і конфліктом розмивається через гібридні впливи, здатність Альянсу

[52] NATO Strategic Communications Policy. Brussels : *NATO*, [б. р.]. URL: https://info.publicintelligence.net/NATO-STRATCOM-Policy.pdf

зберігати цілісність свого інформаційного простору та когнітивну незалежність населення стає визначальною для збереження демократичного ладу та операційної спроможності збройних сил.[53]

Інформаційна стійкість у безпековій політиці НАТО – це не лише технічна захищеність інфраструктури, а комплексна здатність держав-членів, їхніх інституцій та суспільств готуватися до інформаційних шоків, витримувати їх, адаптуватися до мінливих умов та швидко відновлювати функціональність без втрати політичної волі та соціальної єдності. Ця здатність формується під впливом складної системи зовнішніх геополітичних викликів та внутрішніх інституційних і соціокультурних динамік, що вимагає детального аналізу їхньої взаємодії.[54]

Еволюція поняття стійкості в НАТО бере свій початок від Статті 3 Північноатлантичного договору 1949 року, яка зобов'язує сторони «окремо і спільно, шляхом постійної та ефективної самодопомоги та взаємної допомоги підтримувати та розвивати свою індивідуальну та колективну здатність чинити опір збройному нападу». Протягом десятиліть цей обов'язок інтерпретувався переважно у військовому контексті, проте агресія Російської Федерації проти України, починаючи з 2014 року, та посилення системного суперництва з боку Китаю змусили Альянс розширити рамки стійкості на цивільну, технологічну та, перш за все, інформаційну сфери.[55]

У новій Стратегічній концепції 2022 року стійкість визнається критично важливою для виконання основних завдань Альянсу, особливо в контексті протидії авторитарним акторам, які експлуатують відкритість, взаємопов'язаність та цифровізацію демократичних націй. Інформаційна стійкість сьогодні розглядається як інструмент «стримування через

---

[53] NATO. NATO 2022 Strategic Concept. Brussels : *NATO*, 2022. URL: https://www.act.nato.int/wp-content/uploads/2023/05/290622-strategic-concept.pdf

[54] Resilience, Civil Preparedness and Article 3. *NATO*. 13 November 2024. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3

[55] Hall J., Sandeman H. NATO's Resilience: The First and Last Line of Defence. *LSE IDEAS Strategic Update*. London : *LSE IDEAS*, May 2022. URL: https://www.lse.ac.uk/ideas/Assets/Documents/updates/2022-SU-NATO-HallSandeman.pdf

запереченння» (deterrence by denial): якщо супротивник бачить, що суспільство здатне ідентифікувати маніпуляції, а державні інституції зберігають здатність до ефективної комунікації навіть під тиском, стратегічна цінність інформаційних атак нівелюється, що знижує ймовірність їх проведення.[56]

Сучасна модель інформаційної стійкості НАТО базується на чотирьох функціональних стовпах: розумінні, запобіганні, стримуванні та пом'якшенні, а також відновленні. Цей цикл забезпечує системний підхід, де аналіз інформаційного середовища (IEA) дозволяє виявляти загрози на ранніх стадіях, а стратегічні комунікації (StratCom) слугують інструментом проактивного формування наративу. Особливе значення має перехід від реактивного «спростування міфів» до стратегії «pre-bunking» – випереджального інформування населення про можливі тактики маніпуляцій, що створює своєрідний «інформаційний імунітет».[57]

Таблиця 2.1. Складові моделі інформаційної стійкості НАТО

Стовп стійкості	**Функціональний зміст**	**Ключові механізми**
Розуміння (Understand)	Оцінка інформаційного середовища, ідентифікація суб'єктів та їхніх намірів	Модель ABCDE (Актор, Поведінка, Зміст, Ступінь, Ефект), моніторинг медіа.
Запобігання (Prevent)	Зниження вразливості та проактивна комунікація	Медіаграмотність, «pre-bunking», залучення громадянського суспільства.
Стримування/Пом'якшення (Contain/Mitigate)	Нейтралізація активних загроз та обмеження їхнього впливу	Швидке спростування, викриття кампаній впливу, стратегічна прозорість.
Відновлення (Recover)	Оцінка завданої шкоди та адаптація стратегій на основі отриманих уроків	Аналіз TTPs (тактик, технік, процедур) супротивника, вдосконалення доктрин.

Складено за даними.[58]

[56] NATO. NATO 2022 Strategic Concept. Brussels : *NATO*, 2022. URL: https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept

[57] NATO. (n.d.). *NATO's approach to counter information threats* [overview]. https://www.nato.int/en/what-we-do/wider-activities/natos-approach-to-counter-information-threats

[58] RESIST 3: Building Resilience to Information Threats. *UK Government Communications Service.* URL:

Зовнішні фактори, що впливають на інформаційну стійкість НАТО, визначаються глобальним перерозподілом сили та стрімким технологічним розвитком. Росія та Китай як стратегічні конкуренти використовують інформаційний простір для підриву політичної волі Альянсу, експлуатуючи структурні особливості відкритих суспільств.

Російська Федерація визнана найбільш значною та прямою загрозою безпеці Альянсу. Її інформаційна стратегія спрямована на фрагментацію НАТО, підрив довіри до трансатлантичного зв'язку та створення фальшивих наративів про «занепад Заходу». Вплив Росії на інформаційну стійкість Альянсу проявляється через тривале використання «сірих зон» конфлікту, де медійна присутність поєднується з кібератаками та економічним тиском, створюючи кумулятивний ефект дестабілізації. Особливо небезпечною є тактика використання проксі-груп та «сплячих» мереж у соціальних медіа, які активуються в моменти політичних криз або виборчих процесів у країнах НАТО.[59]

Стратегічне вирівнювання Росії та Китаю створює ефект синергії, де обидва актори підтримують ревізіоністські прагнення один одного, змушуючи НАТО розпорошувати ресурси на декілька театрів конкуренції. Китайська підтримка надає Росії технологічну та дипломатичну глибину, що підвищує її стійкість до західного тиску та дозволяє продовжувати агресивні інформаційні кампанії в Європі.[60]

Стрімкий розвиток нових та деструктивних технологій (EDTs) кардинально змінює умови формування інформаційної стійкості. Штучний інтелект (ШІ), квантові обчислення, хмарні технології та 5G мережі створюють

---

https://www.communications.gov.uk/publications/resist-3-building-resilience-to-information-threats/

[59] China–Russia Strategic Alignment and Its Implications for U.S. Global Influence. *Robert Lansing Institute*. 9 March 2026. URL: https://lansinginstitute.org/2026/03/09/china-russia-strategic-alignment-and-its-implications-for-u-s-global-influence/

[60] China–Russia Strategic Alignment and Its Implications for U.S. Global Influence. *Robert Lansing Institute*. 9 March 2026. URL: https://lansinginstitute.org/2026/03/09/china-russia-strategic-alignment-and-its-implications-for-u-s-global-influence/

нові можливості для НАТО, але водночас розширюють поверхню атаки для супротивників.[61]

Таблиця 2.2. Зовнішні чинники впливу на інформаційну стійкість

Фактор	**Механізм впливу**	**Наслідки для НАТО**
Геополітична ревізія	Гібридні атаки, дезінформація, «когнітивна війна»	Підрив політичної єдності, соціальна поляризація.
Системна конкуренція (КНР)	Контроль над інфраструктурою та стандартами, «lawfare»	Технологічна залежність, втрата інформаційної переваги.
Цифрові платформи (Big Tech)	Поширення контенту через непрозорі алгоритми	Формування «ехо-камер», швидка віралізація дезінформації.

Складно за даними.[62]

Фундаментальним внутрішнім чинником інформаційної стійкості є єдність сприйняття загроз. Будь-які тріщини в політичній солідарності – чи то через зростання популізму, економічні розбіжності чи розбіжність поглядів на пріоритетність загроз (Схід проти Півдня) – негайно експлуатуються супротивниками для підриву довіри до колективної оборони. Стійкість зміцнюється через інституціалізацію консультативних норм, що дозволяє Альянсу зберігати «360-градусний підхід» до безпеки.[63]

Важливим аспектом є «стратегічна грамотність» політичних еліт. Наприклад, розуміння ролі ядерного стримування та засобів протидії гібридним впливам дозволяє уникати ситуацій, коли інформаційний шантаж супротивника призводить до паралічу прийняття рішень у межах Північноатлантичної ради.

---

[61] NCI Agency Technology Strategy. Brussels : *NATO Communications and Information Agency*, [б. р.]. URL: https://www.ncia.nato.int/resources/site1/General/newsroom/publications/Public_NCIA_Technology%20Strategy_external_v6%20-%20digital.pdf

[62] Brown W., Kobzova J., Popescu N., Torreblanca J. I. From Shield to Sword: Europe's Offensive Strategy for the Hybrid Age. *European Council on Foreign Relations.* 6 March 2026. URL: https://ecfr.eu/publication/from-shield-to-sword-europes-offensive-strategy-for-the-hybrid-age/

[63] Šenk M., Hynek N. NATO/EU Synergies Against Information Warfare: A "Circulatory Institutionalist" Model of Expert Voluntarism. *European Security.* 2025. URL: https://doi.org/10.1080/ 09662839.2025.2566519

Зміцнення Resolve (рішучості) як одного зі стовпів стримування прямо залежить від здатності лідерів комунікувати складні безпекові питання своїм суспільствам.[64]

Легітимність НАТО в демократичних країнах прямо залежить від підтримки громадян. Тому внутрішнім чинником вразливості є падіння довіри до традиційних інституцій, медіа та експертних спільнот. Інформаційна стійкість суспільства визначається його спроможністю витримувати психологічний тиск та зберігати раціональність у кризових ситуаціях.[65]

Досвід окремих європейських держав, зокрема Фінляндії та Естонії, свідчить, що системний підхід до освіти є одним із найбільш ефективних довгострокових механізмів протидії дезінформації та маніпуляціям у інформаційному середовищі.

У Фінляндії підвищення медіаграмотності населення реалізується через інтеграцію розвитку критичного мислення до національної освітньої програми вже з дошкільного рівня. Така освітня модель спрямована на формування громадян, здатних аналізувати інформацію, розпізнавати маніпулятивні повідомлення та критично оцінювати джерела інформації. У результаті створюється соціальне середовище, у якому пропагандистські або дезінформаційні наративи значно складніше поширюються та впливають на громадську думку.[66]

В Естонії формування інформаційної стійкості базується на поєднанні державної політики та активної участі громадянського суспільства. Зокрема, взаємодія урядових структур із волонтерськими ініціативами, такими як спільнота «Естонські ельфи», сприяє створенню гнучкої системи раннього

---

[64] Nagy T. A. From Assurance to Resilience: Adapting NATO's Nuclear Deterrence Policy. Bratislava : *GLOBSEC Future Security and Defence Council*, 2025. 24 с. URL: https://www.globsec.org/sites/default/files/2025-06/From%20Assurance%20to%20Resilience%20-%20Adapting%20NATO%E2%80%99s%20Nuclear%20Deterrence%20Policy.pdf

[65] NATO's Approach to Counter Information Threats. *NATO*. URL: https://www.nato.int/en/what-we-do/wider-activities/natos-approach-to-counter-information-threats

[66] In Finland, the Battle Against Truly Fake News Starts with Media and AI Literacy in Preschool. *The Reporting Project*. URL: https://www.thereportingproject.org/in-finland-the-battle-against-truly-fake-news-starts-with-media-and-ai-literacy-in-preschool/

виявлення та протидії дезінформаційним кампаніям. Така модель демонструє ефективність мережевої взаємодії держави та суспільства у сфері інформаційної безпеки і значною мірою ґрунтується на високому рівні суспільної довіри до інституцій та механізмів колективної протидії інформаційним загрозам.[67]

Зворотним боком є ситуація в країнах, де роки жорсткої економії та політичної поляризації підірвали соціальний капітал. Без інвестицій у державні сервіси та соціальну інфраструктуру населення стає більш вразливим до популістських наративів, що знижує загальну інформаційну стійкість Альянсу.

Для управління інформаційними чинниками НАТО розбудувало складну інституційну архітектуру. Її ефективність залежить від подолання традиційного поділу на цивільні та військові комунікації (рис. 2.1).

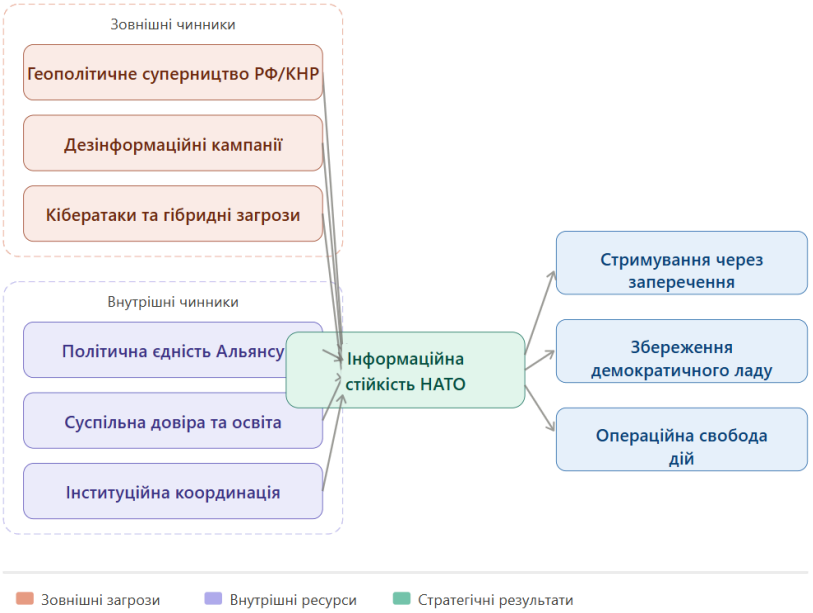


Рисунок 2.1. Взаємодія факторів інформаційної стійкості НАТО

Одним із найбільш перспективних інституційних чинників є концепція «циркуляційного інституціоналізму». Вона передбачає залучення експертів-волонтерів та представників громадянського суспільства до роботи офіційних органів НАТО та ЄС на ротаційній основі. Це дозволяє державним

[67] Šenk M., Hynek N. NATO/EU Synergies Against Information Warfare: A "Circulatory Institutionalist" Model of Expert Voluntarism. *European Security.* 2025. URL: https://www.tandfonline.com/doi/full/10.1080/09662839.2025.2566519

бюрократіям отримувати доступ до сучасних цифрових навичок (OSINT, аналіз соціальних медіа) та підвищує легітимність оборонних ініціатив в очах громадськості.[68]

Таким чином, інформаційна стійкість НАТО формується під впливом взаємодії зовнішніх геополітичних викликів і внутрішніх інституційних та соціальних чинників. Зовнішній тиск, зокрема з боку ревізіоністських держав і швидкий розвиток цифрових технологій, створює нові форми інформаційного протистояння, що спрямовані на підрив політичної єдності Альянсу, маніпуляцію суспільною думкою та послаблення демократичних інститутів. Водночас ефективність протидії таким викликам значною мірою залежить від внутрішньої згуртованості держав-членів, рівня довіри громадян до інституцій, розвитку медіаграмотності та здатності політичних еліт підтримувати стратегічну комунікацію у кризових умовах.

Висновки до Розділу 2

У другому розділі встановлено, що сучасні загрози інформаційній політиці НАТО мають комплексний характер і формуються в умовах зростання ролі інформаційного простору у міжнародних конфліктах. Дезінформація, пропаганда, інформаційні операції та кіберінциденти використовуються як інструменти гібридного впливу, спрямовані на підрив довіри до державних інституцій і поляризацію суспільств. З’ясовано, що дезінформація та інформаційні операції є системними механізмами досягнення політичних і стратегічних цілей, ефективність яких посилюється розвитком цифрових платформ, алгоритмічного поширення контенту та бот-мереж. Водночас НАТО принципово розмежовує дезінформацію і misinformation, що дозволяє формувати відповіді, сумісні з демократичними стандартами. Встановлено, що інформаційна стійкість Альянсу залежить як від зовнішніх чинників стратегічної конкуренції, так і від внутрішніх факторів, зокрема політичної

[68] Šenk M., Hynek N. NATO/EU Synergies Against Information Warfare: A "Circulatory Institutionalist" Model of Expert Voluntarism. *European Security.* 2025. URL: https://www.tandfonline. com/doi/full/10.1080/09662839.2025.2566519

єдності союзників, рівня суспільної довіри та медіаграмотності. Отже, ефективна протидія інформаційним загрозам потребує комплексного підходу, який поєднує стратегічні комунікації, аналітику інформаційного середовища та міжсоюзницьку координацію.

РОЗДІЛ 3
ІНСТРУМЕНТИ ТА МЕХАНІЗМИ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ НАТО

3.1. Стратегічні комунікації як ключовий інструмент інформаційної політики НАТО

Відправною точкою для концептуалізації StratCom є NATO Policy on Strategic Communications, де стратегічні комунікації визначені як скоординоване й доречне використання комунікаційних активностей і спроможностей Альянсу (Public Diplomacy, цивільні та військові Public Affairs, Information Operations, Psychological Operations) на підтримку політик, операцій і діяльності НАТО з метою просування натівських цілей. Документ акцентує, що «сьогоднішнє інформаційне середовище» та сприйняття дій НАТО ключовими аудиторіями можуть прямо впливати на успіх політик і операцій, а отже комунікації мають бути невід'ємною частиною планування, а не реакцією «постфактум» . [69]

Це визначення фіксує StratCom як інтегративний механізм, що має поєднувати стратегічний наратив із практикою реалізації: політична мета → операційне планування → комунікаційна дистрибуція → оцінка ефектів у інформаційному середовищі. У тій самій політиці підкреслюються принципи точності (accuracy), швидкості й реактивності, вимірюваності результативності та максимального охоплення через сукупність натівських каналів.[70]

Як показано на рис. 3.1, стратегічні комунікації НАТО функціонують як інтегрована система, у межах якої політичні цілі, операційне планування та комунікаційні активності поєднуються у єдиний цикл, що завершується оцінкою ефектів у інформаційному середовищі.

---

[69] NATO Strategic Communications Policy. Brussels : *NATO*, [б. р.]. URL: https://info.publicintelligence.net/NATO-STRATCOM-Policy.pdf

[70] NATO Strategic Communications Policy. Brussels : *NATO*, [б. р.]. URL: https://info.publicintelligence.net/NATO-STRATCOM-Policy.pdf

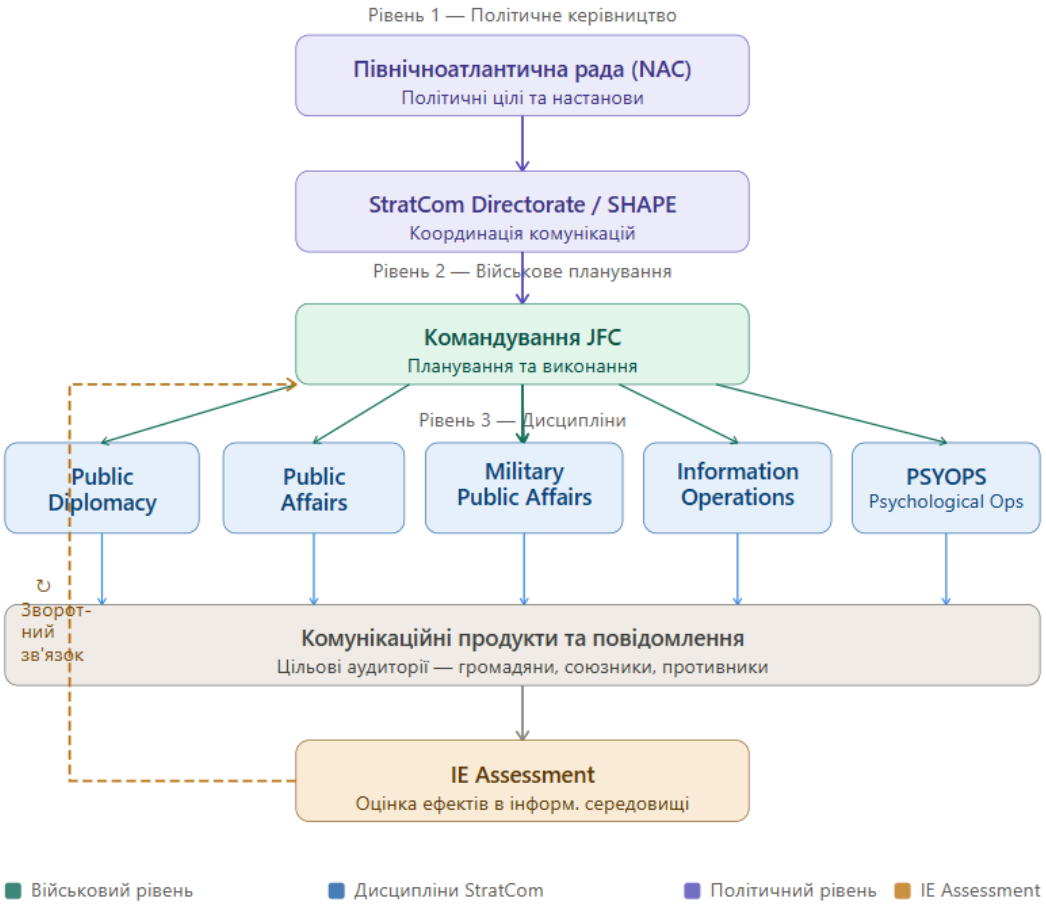


Рисунок 3.1 – Структурна схема інструментів Strategic Communications у НАТО із «золотим ланцюгом» та зворотним зв'язком від оцінки ефектів

Стратегічне значення StratCom додатково підтверджує NATO 2022 Strategic Concept, у якому «disinformation campaigns» розглядаються як елемент гібридних тактик авторитарних акторів, що експлуатують цифровізацію та відкритість демократичних суспільств, а також наголошено на необхідності посилювати стратегічні комунікації як складову стримування та управління стратегічними ризиками. Для контрасту Strategic Concept 2010 відображає попередній етап акцентів: увага була спрямована, зокрема, на зростання кіберзагроз і вразливість критичних комунікаційних мереж, що концептуально підготувало ґрунт для переходу до ширшого бачення інформаційних загроз у 2020-х роках .[71]

[71] NATO 2022 Strategic Concept. Brussels : *NATO, 2022*. URL: https://www.act.nato.int/wp-content/uploads/2023/ 05/290622-strategic-concept.pdf

Інституційний механізм реалізації StratCom у НАТО побудований як політико-військова матриця. North Atlantic Council задає загальний напрям і надає політичні настанови; Генеральний секретар – головний речник і джерело конкретних директив; координацію StratCom у штаб-квартирі здійснює NATO Public Diplomacy Division (за винятком щоденної роботи з медіа, яку веде речник НАТО). Військовий вимір деталізований у політиці MC 0628, яка водночас підкреслює потребу уникати «інформаційного фратрициду» (коли різні інформаційні активності взаємно послаблюють одна одну) та встановлює принципове розмежування між Mil PA й інструментами впливу (PSYOPS/Info Ops), аби не підривати довіру до офіційної комунікації .[72]

На рівні практичних інструментів координація реалізується через «продукти керівництва» та стандарти бренду. В AJP-10 як ключові інструменти напрямного впливу названі NATO Communications Strategy та One NATO Brand Strategy; вони задають єдиний вектор комунікацій і спрямовані на підвищення суспільної довіри у «перевантаженому» цифровому середовищі. У NATO Brand Guide це перетворено на практичну норму: будь-яка публічна дія (включно з «tweet») має підтримувати натівський наратив і впізнаваність, зберігаючи контекст «NATO» під час поширення контенту поза власними платформами . [73]

Окреме місце в інституційній екосистемі StratCom посідає NATO Strategic Communications Centre of Excellence. Центр у Ризі є НАТО-акредитованою міжнародною організацією, але не входить до командної структури НАТО та не підпорядковується іншим натівським органам; його місія – посилювати StratCom-спроможності НАТО, союзників і партнерів, використовуючи міжсекторальну експертизу і сучасні аналітичні підходи. У матеріалах Allied Command Transformation підкреслюється, що Центр функціонує як один із провідних «хабів» аналізу інформаційних загроз, підтримує розвиток доктрини,

---

[72] NATO Strategic Communications Policy. Brussels : *NATO*, [б. р.]. URL: https://info.publicintelligence.net/NATO-STRATCOM-Policy.pdf

[73] UK Ministry of Defence. AJP-10 Allied Joint Doctrine for Strategic Communications. Change 1. London : *UK MoD*, 2023. URL: https://assets.publishing.service.gov.uk/media/6525459d244f8e00138e7343/AJP_10_Strat_Comm_Change_1_web.pdf

тренінги й обмін уроками, а також поєднує дослідницьку діяльність із прикладними потребами практиків .[74]

Показовим прикладом «операціоналізації» StratCom є InfoRange – симулятор інформаційного середовища, який відтворює цифрові канали, мережеві динаміки і поведінку аудиторій та використовується для тренувань від тактичного до стратегічного рівня. У 2024 році InfoRange інтегрували у сценарії Locked Shields, де поруч із кіберзахистом відпрацьовуються правові, управлінські та комунікаційні компоненти криз. Це демонструє зсув від сприйняття стратегічних комунікацій як «пояснення після події» до розуміння їх як елементу комплексної оборони та кризового менеджменту .[75]

Приклади практичного використання StratCom у сучасних кризах доцільно інтерпретувати через рамку «стійкості та легітимності». НАТО прямо пов’язує активізацію протидії інформаційним загрозам зі зростанням ворожої інформаційної активності після незаконної анексії Криму 2014 року. Додатково союзники погодили спільний підхід до counter information threats (схвалено в жовтні 2024 року), який визначає інформаційні загрози як навмисні, шкідливі, маніпулятивні та скоординовані дії (включно з інформаційними операціями і дезінформацією), а також наголошує на принципі фокусування на маніпулятивній поведінці (behavior) і ефектах, а не на цензурі контенту як такій.[76]

Таким чином, StratCom у НАТО є інституційно оформленим механізмом координації, що поєднує публічну дипломатію, медійну комунікацію, інформаційні операції і психологічні компоненти впливу під політичним керівництвом та процедурними обмеженнями довіри. Роль NATO StratCom COE полягає у перетворенні цієї рамки на прикладні спроможності через дослідження, навчання й симуляції; саме така «практична інституціалізація»

---

[74] NATO Strategic Communications Centre of Excellence. *NATO StratCom COE*. URL: https://stratcomcoe.org/

[75] Information Environment Simulation Platform "InfoRange". *NATO StratCom COE*. URL: https://stratcomcoe.org/projects/information-environment-simulation-platform-inforange/3

[76] NATO's Approach to Counter Information Threats. *NATO*. URL: https://www.nato.int/en/what-we-do/wider-activities/natos-approach-to-counter-information-threats

робить StratCom системним інструментом інформаційної політики Альянсу в умовах сучасних загроз.

3.2. Використання цифрових платформ та соціальних мереж у поширенні меседжів

Цифрові платформи стали ключовою інфраструктурою Digital Diplomacy НАТО, оскільки забезпечують прямі канали комунікації з громадськістю союзників і партнерів, швидке поширення офіційних позицій і можливість оперативних спростувань. Офіційні довідкові матеріали для акредитованих медіа фіксують присутність НАТО на головних майданчиках, що виконує функцію «вказівника» на першоджерело в умовах кризи, коли різко зростає ризик фейків і маніпуляцій .[77]

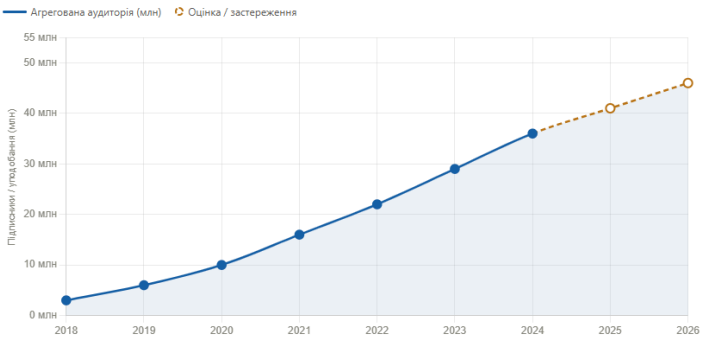
Станом на березень 2026 року масштаби цифрової аудиторії НАТО на провідних платформах можна оцінити так: X – близько 1,99 млн підписників; Facebook – близько 2,39 млн уподобань сторінки; Instagram – близько 2 млн підписників; YouTube – близько 526 тис. підписників; LinkedIn – близько 839 тис. підписників. Ці показники створюють значний «потенціал охоплення», однак не є тотожними реальному впливу, оскільки не враховують перетини аудиторій та алгоритмічні обмеження видимості контенту .[78]

Як показано на рис. 3.2, цифрова аудиторія НАТО демонструє стабільне зростання упродовж останніх років, що свідчить про посилення ролі соціальних платформ у стратегічних комунікаціях Альянсу та розширення потенційного охоплення його інформаційних меседжів.

---

[77] Information for Accredited Media. *NATO News*. 17 квіт. 2023. *NATO*. URL: https://www.nato.int/en/news-and-events/articles/news/2023/04/17/information-for-accredited-media

[78] NATO [@NATO]. Офіційний акаунт НАТО. *X (Twitter)*. URL: https://x.com/NATO



Примітка. Базова точка 2018 р. (~3 млн) – публічна оцінка офіційних платформ НАТО (NATO Annual Report 2018). Значення 2020–2025 рр. відображають приблизну динаміку зростання. Точка 2026 р. (~46 млн) ґрунтується на актуальних показниках ключових платформ (X/Twitter, Facebook, Instagram, YouTube) з урахуванням можливих перетинів аудиторій

Рис. 3.2 – Лінійний графік агрегованої цифрової аудиторії НАТО (2018–2026)

Роль цифрових комунікацій у формуванні публічного іміджу НАТО підтримується брендовою дисципліною. У Brand Guide наголошується, що будь-яка комунікаційна дія формує образ організації, а сторінка про використання контенту та бренду описує One NATO Brand Strategy як засіб підвищення когерентності та впізнаваності натівського контексту поза власними майданчиками. У термінах стратегічних комунікацій це означає інституційну вимогу зберігати єдність наративу, візуальної мови й тональності для зміцнення довіри та опору ворожим наративам.[79]

Таблиця 3.1. Порівняння основних платформ комунікації НАТО (станом на березень 2026 року)

Платформа	**Ключова роль у StratCom**	**Типова комунікаційна функція**	**Базовий ризик**
X (Twitter)	оперативний «порядок денний»	короткі заяви, кризові оновлення, спростування	бот-активність, накрутки, поляризація
Facebook	масова легітимація	довші пояснення, відео, локальні історії	алгоритмічні «бульбашки», групи з дезінформацією
Instagram	візуальна дипломатія	імідж, інфографіка, reels, персоналізація	маніпуляції зображеннями/відео
YouTube	довга форма і «архів»	промови, пресконференції, трансляції	виривання фрагментів з контексту

[79] NATO Brand Guidelines. Brussels : *NATO ACT*, 2023. URL: https://www.act.nato.int/wp-content/uploads/2023/ 06/nato-brand.pdf

LinkedIn	професійна публічна дипломатія	інституційні новини, інновації, кадровий бренд	вузькість аудиторії, репутаційні ризики
Telegram (мовні канали)	нішеві сегменти	адресні повідомлення для мовних груп	конкуренція з пропагандистськими екосистемами

Соціальні мережі застосовуються також для стратегічних повідомлень, кризових комунікацій і протидії дезінформації. НАТО концептуалізує «countering disinformation» як поєднання двох функцій – «розуміти та взаємодіяти» (understand and engage): перша передбачає моніторинг і аналіз, друга – адресну взаємодію з аудиторіями через факти, пояснення і публічні відповіді. Підхід до counter information threats (2024) формалізує цю логіку через визначення загроз і вимогу оцінювати актора, поведінку, контент, ступінь та ефект. [80]

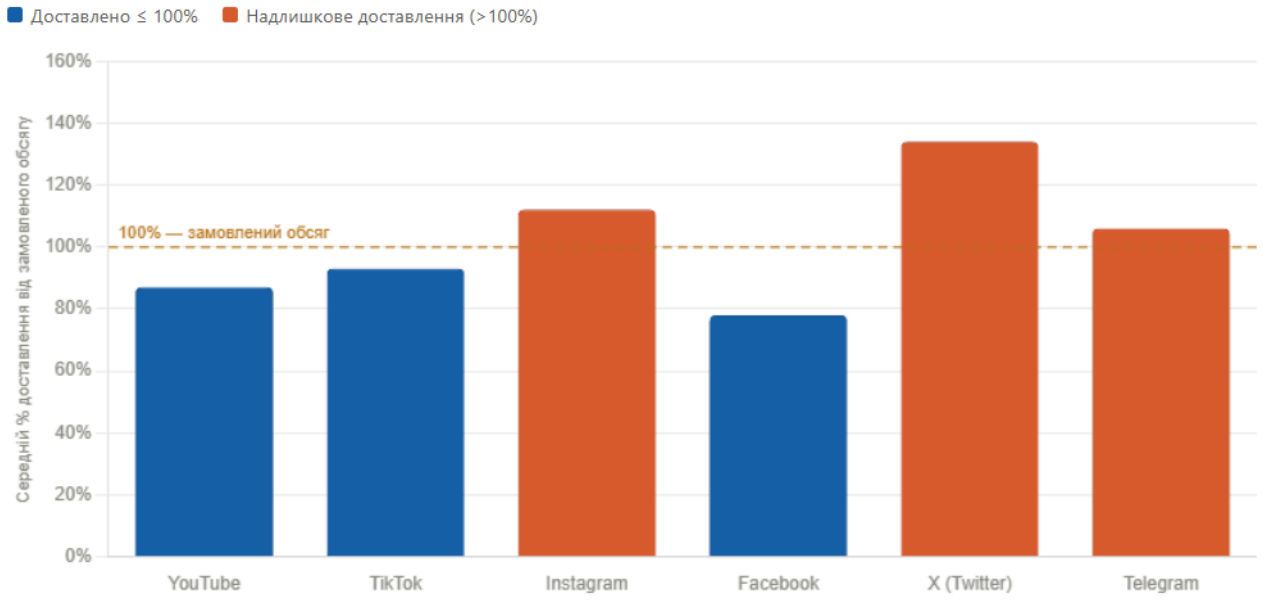
Емпіричний вимір загрози бот-мереж і накруток демонструють дослідження NATO StratCom COE. У звіті Social Media Manipulation for Sale (січень 2026) наголошується, що комерційна маніпуляція неавтентичними взаємодіями лишається широко доступною; при цьому X продемонстрував відносно помітне покращення, видаливши приблизно половину ідентифікованих фейкових акаунтів та взаємодій. Для ілюстрації міжплатформних відмінностей у «доставленні» купленої неавтентичної активності наводяться різко асиметричні показники: одна платформа демонструвала «надлишкове доставлення» фейкових коментарів у середньому на рівні 340% (більше ніж утричі від замовленого), тоді як інша показала менш ніж 1%, а ще одна – 0%. Ці дані релевантні для аналізу Information Operations, оскільки вказують на практичну доступність інфраструктури «штучного посилення» наративів (amplification) через ринок маніпулятивних сервісів.[81]

---

[80] NATO's Approach to Counter Information Threats. *NATO*. URL: https://www.nato.int/cps/ru/natohq/topics_219728.htm

[81] Bergmanis-Korāts G., Haiduchyk T., Smolts B. Social Media Manipulation for Sale: 2025 Experiment on Platform Capabilities to Detect and Counter Inauthentic Social Media Engagement. Riga : *NATO StratCom COE*, 2026. URL: https://stratcomcoe.org/publications/download/Social-Media-Manipulation-FINAL-FILE.pdf

Як показано на рис. 3.3, різні цифрові платформи демонструють значні відмінності у здатності протидіяти маніпулятивним кампаніям, що створює нерівномірний рівень вразливості інформаційного середовища до штучного підсилення дезінформаційних наративів.



Примітка. Значення понад 100% означає «надлишкове доставлення» – постачальники накрутки доставили більше фейкових взаємодій, ніж було замовлено. Пунктирна лінія позначає межу замовленого обсягу (100%). Джерело: Stanford Internet Observatory / «Social Media Manipulation for Sale» (2023).

Рис. 3.3 – Стовпчикова діаграма ефективності доставлення куплених фейкових взаємодій за платформами (за даними «Social Media Manipulation for Sale»)

Оцінювання цифрових кампаній у StratCom доцільно здійснювати через поєднання метрик охоплення, взаємодії та якісних індикаторів зміни знань/ставлень. Публічно доступні фрагменти щорічної звітності НАТО демонструють використання метрик залучення: в одному з описаних кейсів згадується близько 150 тис. взаємодій і охоплення 8,4 млн людей у соціальних мережах. Для дипломного аналізу це важливо як індикатор інституційної нормалізації «вимірюваної комунікації», хоча академічно слід утримуватися від редукції складних політичних ефектів до одних лише engagement-метрик.[82]

[82] The Secretary General's Annual Report 2023. Brussels : *NATO*, 2024. URL: https://www.nato.int/content/dam/nato/legacy-wcm/media_pdf/2024/3/pdf/sgar23-en.pdf

Таблиця 3.2. Інструменти StratCom НАТО та їхня функція в інформаційній політиці

Інструмент	Функція	Механізм реалізації
Public Diplomacy	підтримка довіри та партнерств	публічна взаємодія, форми Digital Diplomacy
Public Affairs / Military PA	інформування і легітимність	брифінги, пояснення дій, медіаробота
Information Operations	інформаційні ефекти у військовому вимірі	планування/оцінка ефектів, інтеграція з операціями
PSYOPS	вплив на поведінку й установки	продукти/активності для затверджених аудиторій
IE Assessment / counter information threats	раннє виявлення маніпуляцій	моніторинг і аналітика актора/поведінки/ефектів
Кампанії та бренд	стандартизація меседжів	One NATO Brand, узгоджені наративи (#WeAreNATO)

Прикладом інформаційної кампанії, спроєктованої саме під цифровий простір, є #WeAreNATO: для неї підготовлено campaign toolkit із настановами щодо наративів, контент-форматів і візуальних рішень, що підтримують повторюваність повідомлень у різних національних контекстах. Функціонально такі кампанії працюють як «парасолькові» меседжі, які одночасно підсилюють єдність і впізнаваність Альянсу та забезпечують рамку для комунікації окремих операцій/навчань, зменшуючи простір для ворожих наративів.[83]

Таким чином, цифрові платформи забезпечують НАТО швидкість і масштаб у комунікації та формують основу Digital Diplomacy й кризового інформування, але одночасно створюють уразливості до комерційних маніпуляцій та бот-мереж. Отже, результативність цифрових комунікацій Альянсу залежить від поєднання брендової дисципліни, процедурної координації StratCom і спроможності аналізувати та нейтралізувати інформаційні загрози, не підриваючи демократичних принципів свободи слова.

[83] WE ARE NATO: Defence and Security Campaign Toolkit. Brussels : *NATO ACT*, 2023. URL: https://www.act.nato. int/wp-content/uploads/2023/06/nato-dsct.pdf

3.3. Співпраця з державами-членами й партнерами у сфері інформаційної безпеки

У сучасній архітектурі міжнародної безпеки інформаційний простір перетворився на повноцінний домен операцій, де межа між миром і конфліктом залишається розмитою, а традиційні методи військового стримування доповнюються стратегіями інформаційної стійкості. Для Організації Північноатлантичного договору співпраця з державами-членами та міжнародними партнерами у цій сфері більше не є допоміжним напрямом дипломатії; вона стала критично важливою складовою виконання трьох основних завдань Альянсу: стримування та оборони, запобігання кризам і врегулювання конфліктів, а також безпеки на основі співпраці. Інституціоналізація цієї співпраці базується на розумінні того, що жодна держава, незалежно від її ресурсного потенціалу, не здатна самостійно протидіяти транскордонним кампаніям дезінформації, кібератакам на критичну інфраструктуру та скоординованим операціям впливу, які експлуатують алгоритмічні вразливості цифрових платформ.

Фундаментом інформаційної політики НАТО є принцип індивідуальної та колективної стійкості, закріплений у Статті 3 Вашингтонського договору. У 2021 році глави держав і урядів Альянсу підтвердили Зобов’язання щодо посилення стійкості (Strengthened Resilience Commitment), яке прямо пов’язує цивільну підготовленість із військовою ефективністю. У межах цього підходу інформаційна безпека розглядається як багатовимірна система, що потребує координації між політичним керівництвом у штаб-квартирі НАТО, національними урядами та профільними структурами .[84]

Ключовим органом, що забезпечує політичну координацію у сфері стратегічних комунікацій (strategic communications) та протидії дезінформації, є Комітет з публічної дипломатії (Committee for Public Diplomacy, CPD). Він слугує основним майданчиком для обміну досвідом між державами-членами та

[84] McInnis K. J., Fata D. P. Pulling Their Weight: The Data on NATO Responsibility Sharing. Washington, D.C. : *CSIS*, 2024. URL: https://www.csis.org/analysis/pulling-their-weight-data-nato-responsibility-sharing

узгодження спільних наративів, що дозволяє уникати явища «інформаційного фратрициду» – ситуації, коли суперечливі повідомлення різних союзників послаблюють загальну стратегічну позицію Альянсу. Додаткову оперативну підтримку надає Група швидкого реагування НАТО (NATO Rapid Response Group, NRRG), яка об'єднує експертів Міжнародного секретаріату та національних фахівців на добровільній основі для раннього попередження про загрози та розробки скоординованих відповідей .[85]

Як видно з табл. 3.3, система інформаційної безпеки НАТО базується на взаємодії політичних, аналітичних і оперативних механізмів координації між союзниками.

Таблиця 3.3. Основні інституційні механізми координації інформаційної безпеки НАТО

Механізм / Орган	**Ключова функція в системі безпеки**	**Основний інструмент взаємодії**
North Atlantic Council (NAC)	Політичне керівництво та стратегічні директиви	Офіційні заяви, декларації самітів
Committee for Public Diplomacy (CPD)	Координація інформаційної політики держав-членів	Регулярні консультації, обмін кращими практиками
NATO Rapid Response Group (NRRG)	Оперативне реагування на інформаційні інциденти	Механізми раннього попередження, спільна атрибуція
Resilience Committee	Моніторинг виконання Статті 3	7 базових вимог до національної стійкості
Joint Intelligence & Security Division	Гібридний аналіз та ситуаційна обізнаність	Розвідувальні брифінги, Hybrid Analysis Branch

У жовтні 2024 року міністри оборони країн НАТО схвалили «Підхід НАТО до протидії інформаційним загрозам» (NATO's approach to counter information threats). Цей документ зафіксував перехід від реактивного спростування окремих фейків до системного аналізу маніпулятивної поведінки (behavior-based approach) акторів. Механізм реалізації цього підходу базується

[85] NATO's Approach to Counter Information Threats : Official text, 18 October 2024. *NATO*. URL: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/10/18/natos-approach-to-counter-information-threats

на чотирьох функціях: розуміння (Understand), запобігання (Prevent), стримування та пом’якшення (Contain & Mitigate), а також відновлення (Recover) .[86]

Роль держав-членів у зміцненні інформаційної безпеки Альянсу полягає не лише у виконанні спільних директив, а й у розвитку національних спроможностей, які можуть бути інтегровані в загальну систему оборони. Прикладом такої інтеграції є участь національних центрів кібербезпеки та стратегічних комунікацій у мережі обміну даними NATO Enterprise. Важливим аспектом є також узгодження національного законодавства з вимогами щодо захисту критичної інформаційної інфраструктури, зокрема мереж 5G та підводних кабелів. У 2025 році Альянс запустив нову військову активність «Baltic Sentry», спрямовану на посилення присутності в Балтійському морі та покращення здатності реагувати на дестабілізуючі акти, включно з інформаційно-психологічними операціями в регіоні .[87]

Особливе значення має впровадження штучного інтелекту (AI) для аналізу інформаційного середовища (IEA). НАТО створила Спеціальну групу з питань інформаційних операцій на основі ШІ та дипфейків (Task Force on AI-enabled Information Operations and Deep Fakes), щоб підготувати союзників до нових типів маніпуляцій. Це демонструє зсув у бік технологізації співпраці, де обмін алгоритмами та аналітичними моделями стає таким же важливим, як і обмін політичними деклараціями .[88]

Важливою складовою екосистеми інформаційної безпеки НАТО є центри передового досвіду (Centres of Excellence, COE). Хоча вони формально не входять до командної структури Альянсу, їхня роль у забезпеченні інтелектуальної переваги та підготовці кадрів є визначальною. Центр стратегічних комунікацій НАТО (NATO StratCom COE) у Ризі виступає

---

[86] What is NATO's Approach to Counter Information Threats? : інформаційний листок. Brussels : *NATO*, 2024. URL: https://www.nato.int/content/dam/nato/legacy-wcm/media_pdf/2024/12/pdf/2412-Information-Threats.pdf

[87] The Secretary General's Annual Report 2024. Brussels : *NATO,* 2025. URL: https://www.nato.int/content/dam/nato/legacy-wcm/media_pdf/2025/4/pdf/sgar24-en.pdf

[88] The Secretary General's Annual Report 2024. Brussels : *NATO,* 2025. URL: https://www.nato.int/content/dam/nato/legacy-wcm/media_pdf/2025/4/pdf/sgar24-en.pdf

провідним хабом, який об’єднує представників держав-членів для розробки доктрин та проведення досліджень. У 2024 році Центр опублікував першу доктрину фундаментальних принципів стратегічних комунікацій, яка стала спільним стандартом для професіоналів усього Альянсу .[89]

Взаємодія між Центром у Ризі та національними інституціями реалізується через спільні проєкти, такі як «Social Media Manipulation for Sale», що дозволяє оцінювати вразливість демократичних суспільств до комерційних маніпуляцій. Іншим критично важливим об’єктом є Об’єднаний центр передового досвіду з кібероборони (CCDCOE) у Таллінні, який забезпечує технічну складову інформаційної безпеки. Оскільки гібридні загрози часто поєднують кібератаки з дезінформацією, координація між цими двома центрами дозволяє Альянсу бачити цілісну картину ворожих операцій .[90]

У 2025 році було створено нову посаду Спеціального координатора з питань гібридних загроз (Special Coordinator for Hybrid Threats), що стало відповіддю на потребу в посиленні горизонтальних зв’язків між різними структурами НАТО, від військових штабів до цивільних агентств. Цей крок відображає тенденцію до централізації управління у сфері, яка раніше була розпорошена між різними департаментами .[91]

Таблиця 3.4. Центри передового досвіду та їхній внесок у інформаційну безпеку (2024–2025 рр.)

Центр передового досвіду	**Місцезнаходження**	**Ключовий внесок у співпрацю**	**Основні проекти 2025 року**
StratCom COE	Рига, Латвія	Доктринальна база, аналіз ШІ в комунікаціях	AI Laboratory, NextGen Information Environment

[89] Shaping the Future of Strategic Communications in NATO. *NATO ACT*. 2025. URL: https://www.act.nato.int/article/stratcom-coe-2025/

[90] Munteanu N. A. NATO's Mechanisms for the Governance of Cybersecurity. *Studia Securitatis*. 2025. *Vol. 19*, № 1. P. 208—217. URL: https://doi.org/10.54989/stusec.2025.19.01.15

[91] Countering Hybrid Threats. Updated: 29 January 2026. *NATO*. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

CCDCOE	Таллінн, Естонія	Технічна стійкість, юридична атрибуція кібератак	Locked Shields 2025, Tallinn Manual 2.0
Hybrid COE	Гельсінкі, Фінляндія	Платформа для взаємодії НАТО–ЄС	Hybrid Fusion Cell, PROTEUS Program
Energy Security COE	Вільнюс, Литва	Захист енергетичної інформаційної інфраструктури	Аналіз кіберзагроз для енергомереж

Як показано в табл. 3.4, центри передового досвіду відіграють ключову роль у розвитку аналітичних і технічних спроможностей НАТО у сфері інформаційної та кібербезпеки.

Особливу роль у системі партнерської взаємодії відіграє Спільний центр аналізу, підготовки та навчання НАТО-Україна (JATEC) у Бидгощі (Польща), який розпочав роботу в лютому 2025 року. JATEC став першою спільною інституцією такого типу, де персонал НАТО та України працює як єдина команда. Центр фокусується на п’яти напрямах: військовий розвиток, цифровізація, освіта, комплексна оборона та трансформація й інтероперабельність (interoperability). Цей механізм дозволяє Альянсу в реальному часі імпортувати український досвід протидії високотехнологічному агресору, зокрема у сферах ШІ-аналітики, боротьби з дезінформацією та захисту цифрової інфраструктури від кібер-кінетичних ударів .[92]

Співпраця з Україною в межах JATEC демонструє перехід до моделі «швидкої адаптації». Як зазначив старший національний представник України полковник Валерій Вишнівський, швидкість навчання є вирішальним фактором сучасної війни, і JATEC слугує мостом, який дозволяє НАТО скоротити цикли адаптації доктрин з років до місяців або навіть тижнів. У 2025 році JATEC організував три інноваційні виклики для України, результати яких – наприклад, рішення для наведення БПЛА на основі ШІ – безпосередньо посилюють спроможності обох сторін .[93]

---

[92] NATO–Ukraine Joint Analysis, Training and Education Centre Opens! *Polish Ministry of National Defence*. 2025. URL: https://www.gov.pl/web/national-defence/nato--ukraine-joint-analysis-training-and-education-centre-opens

[93] One Year of JATEC: Strengthening Ukraine–NATO Cooperation and Innovation. *The Odessa Journal*. 2025. URL:

Взаємодія НАТО з Європейським Союзом є наріжним каменем європейської архітектури безпеки. Станом на 2025 рік обидві організації мають 23 спільних члени, що обумовлює необхідність повної координації зусиль для уникнення дублювання та ефективного використання обмежених ресурсів. Співпраця реалізується через Спільну декларацію та регулярні звіти про прогрес. 10-й звіт (червень 2025 р.) зафіксував значне посилення політичного діалогу та практичної координації у сферах мобільності, кібербезпеки та протидії гібридним загрозам .[94]

Одним із найбільш успішних інструментів є Європейський центр з протидії гібридним загрозам (Hybrid CoE) у Гельсінкі. Він забезпечує аналітичну підтримку як для НАТО, так і для ЄС, функціонуючи як інтелектуальний міст. У межах ЄС також діє Гібридний аналітичний відділ (EU Hybrid Fusion Cell), інтегрований у структуру Розвідувального та ситуаційного центру ЄС (INTCEN), який тісно співпрацює з аналогічними структурами в НАТО. Така мережева структура дозволяє ідентифікувати ворожі операції, що охоплюють кілька країн та доменів одночасно .[95]

Табл. 3.5 демонструє, що співпраця НАТО та ЄС охоплює стратегічні комунікації, кіберзахист і протидію гібридним загрозам.

Таблиця 3.5. Основні напрями співпраці НАТО та Європейського Союзу у сфері інформаційної безпеки

Сфера взаємодії	**Формат співпраці НАТО–ЄС**	**Конкретний результат (2024–2025 рр.)**
Кібербезпека	Структурований діалог з питань кіберпростору	Спільні заяви із засудженням зловмисної кібердіяльності
Гібридні загрози	Робоча група зі стійкості критичної інфраструктури	Оцінка вразливостей підводних кабелів у Балтиці

https://odessa-journal.com/one-year-of-jatec-strengthening-ukraine-nato-cooperation-and-innovation

[94] EU–NATO Strategic Partnership. *European External Action Service*. URL: https://www.eeas.europa.eu/eeas/eu-nato-strategic-partnership_en

[95] Brunet B. Strengthening Europe's Actions Against Hybrid Threats: Setting Up a Proteus Programme : GPC Policy Brief. Madrid : *IE University Global Policy Centre*, 2025. URL: https://docs.ie.edu/GPC/3_AAFF_short%20CGP_Strengthening%20Europe%27s.pdf

Стратегічні комунікації	Експертні обміни на рівні штабів	Узгодження наративів щодо підтримки України та протидії РФ
Навчання	Паралельні та координовані навчання (PACE)	EU Integrated Resolve 2024 та NATO CMX 2025

Крім ЄС, НАТО розвиває співпрацю з глобальними партнерами, зокрема з країнами «Індо-Тихоокеанської четвірки» (Австралія, Японія, Південна Корея, Нова Зеландія). Це зумовлено зростаючим вирівнюванням стратегічних цілей Росії, Китаю, Ірану та КНДР, що вимагає глобального підходу до інформаційної безпеки. У липні 2024 року НАТО оголосила про створення офісу зв'язку в Йорданії, що посилило взаємодію з партнерами на Південному фланзі .[96]

Процес формування єдиного інформаційного простору безпеки неможливий без регулярних тренувань та перевірки навичок у режимі реального часу. Навчання «Locked Shields», які проводить CCDCOE, є вершиною такої співпраці. У 2025 році вони об'єднали понад 4000 експертів з 41 країни, які захищали віртуалізовані національні системи (енергомережі, супутникові канали, мережі 5G) від понад 9000 комплексних атак. Особливістю Locked Shields 2025 стало впровадження квантових обчислень та наративів на основі ШІ, що змушувало команди працювати не лише в технічному, а й у стратегічному та правовому доменах .[97]

Успіх у Locked Shields 2025 продемонстрували багатонаціональні команди: перше місце посіла збірна Німеччини та Сінгапуру, друге – Польщі та Франції, третє – Італії, Словенії та США (Національна гвардія Колорадо). Це підкреслює, що інтероперабельність (interoperability) досягається саме через здатність фахівців з різних країн працювати як єдиний організм під час гострої кризи .[98]

---

[96] The Secretary General's Annual Report 2024. Brussels : *NATO,* 2025. URL: https://www.nato.int/content/dam/nato/legacy-wcm/media_pdf/2025/4/pdf/sgar24-en.pdf

[97] Locked Shields 2025 Showcased Nations' Commitment to Defending Cyberspace. *CCDCOE*. 2025. URL: https://ccdcoe.org/news/2025/locked-shields-2025-showcased-nations-commitment-to-defending-cyberspace/

[98] Locked Shields 2025 Showcased Nations' Commitment to Defending Cyberspace. *CCDCOE*. 2025. URL:

Іншим важливим інструментом є симулятор інформаційного середовища «InfoRange», розроблений StratCom COE. Він дозволяє відтворювати цифрові канали та поведінку аудиторій, що використовується для тренувань від тактичного до стратегічного рівня. У 2024 році InfoRange інтегрували в сценарії навчань, де поруч із кіберзахистом відпрацьовувалися правові та комунікаційні компоненти. На 2026 рік заплановано навчання «Synesis», які стануть першим досвідом використання AI-агентів для моделювання реакцій великих груп населення на інформаційні операції .[99]

Як видно з табл. 3.6, спільні навчання та програми НАТО сприяють підвищенню інтероперабельності та координації союзників у сфері інформаційної безпеки.

Таблиця 3.6. Ключові програми та навчання НАТО у сфері інформаційної та кібербезпеки

Програма / Навчання	**Ключова мета у сфері безпеки**	**Масштаб та учасники**
Locked Shields	Жива кібероборона та стратегічне управління	4000+ експертів, 41 нація, приватний сектор
Cyber Coalition	Перевірка процедур колективної оборони в кіберпросторі	Командно-штабні навчання, органи НАТО, союзники
StratCom LiveEX	Репетиція крос-секторальних відповідей на інфо-загрози	Політики, військові комунікатори, цивільні експерти
#WeAreNATO	Підвищення суспільної довіри та впізнаваності Альянсу	Публічна дипломатія, цифрові кампанії в соцмережах
JATEC Innovation Challenges	Спільна розробка технологічних рішень для фронту	Стартапи, інвестори, військові НАТО та України

Важливу роль у підготовці кадрів відіграє також освітній напрям. StratCom COE пропонує онлайн-курс «Introduction to Strategic Communications», а CCDCOE виступає головним департаментом НАТО з питань навчання

https://ccdcoe.org/news/2025/locked-shields-2025-showcased-nations-commitment-to-defending-cyberspace/

[99]Exercise Synesis 2026. *NATO StratCom COE*. URL: https://stratcomcoe.org/projects/exercise-synesis-2026/4

операціям кіберзахисту. Це створює спільну професійну мову та уніфіковане розуміння загроз серед офіцерів та державних службовців країн Альянсу.

Таким чином, співпраця з державами-членами та партнерами у сфері інформаційної безпеки пройшла шлях від допоміжної функції до ключового елемента колективної оборони НАТО. У сучасних умовах інформаційна стійкість Альянсу базується не на централізованому управлінні, а на складній мережевій взаємодії між штаб-квартирою, національними урядами, центрами передового досвіду та міжнародними організаціями, такими як ЄС та G7. Інтеграція партнерів, зокрема України, через такі механізми, як JATEC, дозволяє НАТО залишатися на передньому краї технологічних інновацій та оперативно адаптуватися до нових викликів. Проте, ефективність цієї архітектури безпеки надалі залежатиме від здатності союзників подолати ресурсну асиметрію, узгодити правові рамки та забезпечити політичну єдність перед обличчям скоординованих гібридних атак. Тільки поєднання технічної переваги з високим рівнем суспільної довіри та медіаграмотності дозволить Альянсу зберегти свою цілісність у цифрову епоху.

Висновки до Розділу 3

У третьому розділі встановлено, що інформаційна політика НАТО реалізується через систему взаємопов’язаних інструментів, які поєднують стратегічні комунікації, цифрові платформи та співпрацю з державами-членами і партнерами. Сучасний підхід Альянсу передбачає інтеграцію комунікацій у політичне й операційне планування, що робить їх важливою складовою стримування та кризового менеджменту. Доведено, що ключовим інструментом інформаційної політики є стратегічні комунікації (StratCom), які забезпечують узгоджене використання публічної дипломатії, зв’язків із громадськістю та інформаційних операцій для підтримки політичних і військових цілей НАТО. З’ясовано, що цифрові платформи стали важливим каналом поширення меседжів Альянсу, водночас створюючи нові ризики, пов’язані з маніпуляціями та дезінформацією. Ефективність комунікацій залежить від узгодженості

стратегічних наративів, аналітики інформаційного середовища та оцінки впливу на аудиторії. Отже, інформаційна політика НАТО ґрунтується на поєднанні стратегічних комунікацій, цифрових інструментів і міжнародної співпраці, що дозволяє Альянсу підвищувати стійкість до інформаційних загроз і підтримувати реалізацію своїх безпекових цілей.

ВИСНОВКИ

У результаті проведеного дослідження було проаналізовано теоретичні та практичні аспекти реалізації інформаційної політики НАТО в умовах сучасних загроз. Робота була спрямована на вивчення ролі інформаційного виміру у системі міжнародної безпеки, дослідження інституційних механізмів і комунікаційних інструментів Альянсу, а також визначення основних викликів, пов’язаних із поширенням дезінформації та гібридних форм впливу. Проведений аналіз дозволив комплексно розглянути еволюцію інформаційної політики НАТО, її інституційні засади та сучасні механізми реалізації.

У ході дослідження встановлено, що інформаційна політика є важливим елементом сучасної системи міжнародної безпеки та охоплює комплекс політичних, комунікаційних і технологічних заходів, спрямованих на формування, поширення та захист інформації. У сучасному міжнародному середовищі інформаційна політика відіграє значну роль у реалізації державних і міжнародних інтересів, оскільки інформаційний простір став одним із ключових вимірів глобальної конкуренції. Інформаційні процеси безпосередньо впливають на формування суспільної думки, легітимність політичних рішень та стабільність міжнародних відносин. У зв’язку з цим інформаційна політика дедалі частіше розглядається як складова безпекової політики, що поєднує елементи публічної дипломатії, стратегічних комунікацій, інформаційної безпеки та протидії дезінформації.

Проведений аналіз показав, що інформаційна політика НАТО зазнала значної трансформації впродовж свого розвитку. У період Холодної війни комунікаційна діяльність Альянсу була спрямована переважно на інформування громадськості про його оборонну роль та забезпечення підтримки колективної безпеки. Після завершення Холодної війни та розширення спектра загроз інформаційна політика НАТО поступово еволюціонувала в комплексну систему стратегічних комунікацій. На сучасному етапі вона базується на принципах достовірності, прозорості, узгодженості повідомлень, оперативності комунікації

та міжінституційної координації. Особливу увагу приділяється інтеграції різних комунікаційних інструментів, включно з публічною дипломатією, зв’язками із засобами масової інформації, інформаційними операціями та цифровими комунікаціями. Такий підхід дозволяє Альянсу ефективно реагувати на виклики сучасного інформаційного середовища.

У результаті дослідження встановлено, що реалізація інформаційної політики НАТО забезпечується розгалуженою інституційною системою, до якої входять політичні органи, військові структури та спеціалізовані комунікаційні підрозділи. Ключову роль у формуванні інформаційної політики відіграє Північноатлантична рада, яка визначає загальні напрями комунікаційної діяльності Альянсу. Важливими елементами цієї системи є Міжнародний секретаріат НАТО, підрозділи публічної дипломатії, військові командування, а також аналітичні та дослідницькі центри, зокрема Центр передового досвіду зі стратегічних комунікацій. Основними напрямами інформаційної діяльності Альянсу є стратегічні комунікації, публічна дипломатія, інформаційна підтримка військових операцій, протидія дезінформації та розвиток міжнародної співпраці у сфері інформаційної безпеки.

Дослідження показало, що сучасні міжнародні конфлікти дедалі частіше набувають гібридного характеру та поєднують військові й невійськові методи впливу. У межах таких конфліктів інформаційний компонент відіграє ключову роль, оскільки інформаційні операції, дезінформаційні кампанії, кібератаки та психологічні методи впливу використовуються для досягнення політичних і стратегічних цілей. Гібридні загрози спрямовані на підрив довіри до державних інституцій, посилення соціальної поляризації та дестабілізацію політичних систем. Особливістю сучасних інформаційних загроз є їхній транскордонний характер, висока швидкість поширення та складність ідентифікації джерел впливу. У таких умовах інформаційний простір перетворюється на важливий елемент стратегічної конкуренції між державами.

У ході дослідження встановлено, що дезінформація, пропаганда та інформаційні операції є ключовими інструментами сучасного інформаційного

протистояння. Їх застосування спрямоване на формування вигідних політичних наративів, маніпулювання громадською думкою та дискредитацію політичних опонентів. Розвиток цифрових технологій, соціальних мереж та алгоритмічних систем поширення інформації значно розширив можливості проведення таких інформаційних кампаній. У сучасних умовах інформаційні операції можуть поєднувати традиційні пропагандистські методи з новими технологічними інструментами, включно з використанням бот-мереж, фейкових акаунтів та систем мікротаргетингу. Це значно підвищує ефективність інформаційного впливу та ускладнює процес протидії таким загрозам.

Встановлено, що стратегічні комунікації є одним із ключових механізмів реалізації інформаційної політики НАТО. Вони передбачають узгоджене використання різних комунікаційних інструментів і каналів для досягнення політичних і безпекових цілей Альянсу. До основних інструментів стратегічних комунікацій належать публічна дипломатія, робота із засобами масової інформації, інформаційна підтримка військових операцій, а також активне використання цифрових платформ і соціальних мереж. Використання сучасних комунікаційних технологій дозволяє НАТО оперативно поширювати інформацію, формувати позитивний міжнародний імідж та ефективно реагувати на інформаційні загрози. Особливе значення має проактивна комунікаційна політика, спрямована на формування довіри до діяльності Альянсу та зміцнення інформаційної стійкості суспільств.

Результати дослідження свідчать, що ефективна реалізація інформаційної політики НАТО значною мірою залежить від рівня координації між державами-членами та міжнародними партнерами. Спільні інформаційні програми, обмін досвідом, проведення спільних навчань і координація стратегічних комунікацій сприяють підвищенню стійкості союзників до інформаційних та гібридних загроз. Важливу роль відіграє співпраця НАТО з іншими міжнародними організаціями, зокрема Європейським Союзом, у сфері протидії дезінформації та інформаційним маніпуляціям. Така взаємодія дозволяє формувати комплексний підхід до забезпечення інформаційної безпеки

та зміцнювати колективну стійкість демократичних суспільств до зовнішніх інформаційних впливів.

Таким чином, проведене дослідження підтвердило, що інформаційна політика НАТО є важливою складовою сучасної системи міжнародної безпеки та відіграє значну роль у протидії інформаційним і гібридним загрозам. Сучасні умови розвитку міжнародних відносин характеризуються зростанням ролі інформаційного простору як одного з ключових напрямів стратегічної конкуренції між державами. У зв’язку з цим НАТО активно розвиває систему стратегічних комунікацій, удосконалює інституційні механізми координації інформаційної діяльності та розширює співпрацю з державами-членами і партнерами у сфері інформаційної безпеки. Ефективне використання комунікаційних інструментів, цифрових платформ та міжнародної координації дозволяє Альянсу підвищувати стійкість демократичних суспільств до інформаційних впливів і зміцнювати стабільність міжнародного безпекового середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Боднар А. О. *Міжнародна інформаційна безпека* : кваліфікаційна робота. Вінниця : Донецький національний університет ім. В. Стуса, 2020. 82 с. URL: https://jarch.donnu.edu.ua/article/view/9490

2. Васютіна В. В. *Інформаційна політика України в контексті євроінтеграційних процесів* : дис. … канд. політ. наук : 23.00.02. Одеса, 2014. 234 с. URL: http://dspace.pdpu.edu.ua/handle/123456789/327

3. Коротаєв С. Р. Правові аспекти інформаційного поля України. Національна інформаційна політика. *Актуальні проблеми міжнародних відносин*. Київ, 1997. Вип. 3, ч. 2. С. 58–63.

4. AJP-10: Allied Joint Doctrine for Strategic Communications. Change 1. London : *UK Ministry of Defence*, 2023. URL: https://assets.publishing.service.gov.uk/media/6525459d244f8e00138e7343/AJP_10_Strat_Comm_Change_1_web.pdf

5. Bergmanis-Korāts G., Haiduchyk T., Smolts B. Social Media Manipulation for Sale: 2025 Experiment on Platform Capabilities to Detect and Counter Inauthentic Social Media Engagement. Riga : NATO StratCom COE, 2026. URL: https://stratcomcoe.org/publications/download/Social-Media-Manipulation-FINAL-FILE.pdf

6. Brown W., Kobzova J., Popescu N., Torreblanca J. I. From Shield to Sword: Europe's Offensive Strategy for the Hybrid Age. *European Council on Foreign Relations.* 6 March 2026. URL: https://ecfr.eu/publication/from-shield-to-sword-europes-offensive-strategy-for-the-hybrid-age/

7. Brunet B. Strengthening Europe's Actions Against Hybrid Threats: Setting Up a Proteus Programme : GPC Policy Brief. Madrid : IE University Global Policy Centre, 2025. URL: https://docs.ie.edu/GPC/3_AAFF_short%20CGP_Strengthening%20Europe%27s.pdf

8. Bucharest Summit Declaration : Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Bucharest on 3 April 2008. Brussels : *NATO*, 2008. URL: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2008/04/03/bucharest-summit-declaration

9. China–Russia Strategic Alignment and Its Implications for U.S. Global Influence. *Robert Lansing Institute*. 9 March 2026. URL: https://lansinginstitute.org/2026/03/09/china-russia-strategic-alignment-and-its-implications-for-u-s-global-influence/

10. Cognitive Warfare. *NATO ACT*. URL: https://www.act.nato.int/activities/cognitive-warfare/

11. Countering Hybrid Threats. Updated: 29 January 2026. *NATO*. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

12. Strategic communication and countering foreign information manipulation and interference. *European Commission*. URL: https://commission.europa.eu/topics/countering-information-manipulation_en

13. Cyber Defence. *NATO*. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence

14. EU–NATO Strategic Partnership. *European External Action Service*. URL: https://www.eeas.europa.eu/eeas/eu-nato-strategic-partnership_en

15. Exercise Synesis 2026. *NATO StratCom COE*. URL: https://stratcomcoe.org/projects/exercise-synesis-2026/4

16. Foreign Office Minister Condemns Russia for NotPetya Attacks. *UK Foreign & Commonwealth Office*. URL: https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks

17. Fredheim R., Bay S., Haiduchyk T., Dek A., Stolze M. Social Media Manipulation 2022/2023 : Assessing the Ability of Social Media Companies to Combat Platform Manipulation. Riga : NATO StratCom COE, 2023. URL:

https://stratcomcoe.org/publications/download/Social-Media-Manipulation-2022-2023-DIGITAL.pdf

18. Güleç C. NATO and Public Diplomacy: Opportunities and Constraints of 21st Century. *Perceptions*. 2021. Vol. XXVI, № 1. P. 100–120. URL: https://dergipark.org.tr/tr/download/article-file/1905361

19. Hall J., Sandeman H. NATO's Resilience: The First and Last Line of Defence. LSE IDEAS Strategic Update. London : LSE IDEAS, May 2022. URL: https://www.lse.ac.uk/ideas/Assets/Documents/updates/2022-SU-NATO-HallSandeman.pdf

20. How Does NATO Respond to Disinformation? *NATO News*. 25 May 2021. *NATO*. URL: https://www.nato.int/en/news-and-events/articles/news/2021/05/25/how-does-nato-respond-to-disinformation

21. In Finland, the Battle Against Truly Fake News Starts with Media and AI Literacy in Preschool. *The Reporting Project*. URL: https://www.thereportingproject.org/in-finland-the-battle-against-truly-fake-news-starts-with-media-and-ai-literacy-in-preschool/

22. Information Environment Simulation Platform "InfoRange". *NATO StratCom COE*. URL: https://stratcomcoe.org/projects/information-environment-simulation-platform-inforange/3

23. Information for Accredited Media. *NATO News*. 17 квіт. 2023. *NATO*. URL: https://www.nato.int/en/news-and-events/articles/news/2023/04/17/information-for-accredited-media

24. Joint Air Power Competence Centre. C-UAS Strategic Communications. *JAPCC*. [б. р.]. URL: https://www.japcc.org/chapters/c-uas-strategic-communications/

25. Joseph S. Nye, Jr. Public Diplomacy and Soft Power. *Public Diplomacy in a Changing World*. 2008. Vol. 616. P. 94-109. https://www.jstor.org/stable/25097996?read-now=1&seq=3

26. Letzing J. What Is Information Warfare and How Pervasive Is It? *World Economic Forum*. 14 April 2022. URL: https://www.weforum.org/stories/2022/04/what-is-information-warfare-and-how-pervasive-is-it/

27. Locked Shields 2025 Showcased Nations' Commitment to Defending Cyberspace. *CCDCOE*. 2025. URL: https://ccdcoe.org/news/2025/locked-shields-2025-showcased-nations-commitment-to-defending-cyberspace/

28. McInnis K. J., Fata D. P. Pulling Their Weight: The Data on NATO Responsibility Sharing. Washington, D.C. : CSIS, 2024. URL: https://www.csis.org/analysis/pulling-their-weight-data-nato-responsibility-sharing

29. Munteanu N. A. NATO's Mechanisms for the Governance of Cybersecurity. *Studia Securitatis*. 2025. Vol. 19, № 1. P. 208—217. DOI: 10.54989/stusec. 2025.19.01.15

30. Nagy T. A. From Assurance to Resilience: Adapting NATO's Nuclear Deterrence Policy. Bratislava : GLOBSEC Future Security and Defence Council, 2025. 24 p. URL: https://www.globsec.org/sites/default/files/2025-06/From%20Assurance%20to%20Resilience%20-%20Adapting%20NATO%E2%80%99s%20Nuclear%20Deterrence%20Policy.pdf

31. NATO [@NATO]. Офіційний акаунт НАТО. *X (Twitter)*. URL: https://x.com/NATO

32. NATO 2022 Strategic Concept. Brussels : *NATO, 2022*. URL: https://www.act.nato.int/wp-content/uploads/2023/05/290622-strategic-concept.pdf

33. NATO ACT. NATO StratCom COE. *ACT NATO*. [б. р.]. URL: https://www.act.nato.int/article/nato-stratcom-coe/

34. NATO ACT. StratCom COE 2024. *ACT NATO*. 2024. URL: https://www.act.nato.int/article/stratcom-coe-2024/

35. NATO Brand Guidelines. Brussels : *NATO ACT*, 2023. URL: https://www.act.nato.int/wp-content/uploads/2023/06/nato-brand.pdf

36. NATO Defence College. Research Division. Rome : *NDC*, [б. р.]. URL: https://www.ndc.nato.int/research/

37. NATO Strategic Communications Centre of Excellence. *NATO StratCom COE*. URL: https://stratcomcoe.org/

38. NATO Strategic Communications Policy. Brussels : NATO, [б. р.]. URL: https://info.publicintelligence.net/NATO-STRATCOM-Policy.pdf

39. NATO–Ukraine Joint Analysis, Training and Education Centre Opens! *Polish Ministry of National Defence*. 2025. URL: https://www.gov.pl/web/national-defence/nato--ukraine-joint-analysis-training-and-education-centre-opens

40. NATO. Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of NATO. Brussels : NATO, 2010. URL: https://www.nato.int/content/dam/nato/legacy-wcm/media_pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

41. NATO. AJP-3.10 Allied Joint Doctrine for Information Operations. Ed. A, Ver. 1. Brussels : NATO, 2019. URL: https://mpsotc.army.gr/wp-content/uploads/2024/03/2.-AJP-3.10-EDA-V1-E.pdf

42. NATO. Allied Command Operations (ACO). Brussels : NATO, [б. р.]. URL: https://www.nato.int/en/about-us/organization/nato-structure/allied-command-operations-aco

43. NATO. Bucharest Summit Declaration. Brussels : NATO, 2008. URL: https://www.nato.int/cps/en/natolive/official_texts_46247.htm

44. NATO. Committee on Public Diplomacy (CPD). Brussels : NATO, [б. р.]. URL:

https://www.nato.int/en/about-us/organization/nato-structure/committee-on-public-diplomacy-cpd

45. NATO. Countering Hybrid Threats. Brussels : NATO, [б. p.]. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

46. NATO. NATO 2022 Strategic Concept. Brussels : NATO, 2022. URL: https://www.act.nato.int/wp-content/uploads/2023/05/290622-strategic-concept.pdf

47. NATO. NATO Communications and Information Agency (NCI Agency). Brussels : NATO, [б. p.]. URL: https://www.nato.int/en/about-us/organization/nato-structure/nato-communications-and-information-agency-nci-agency

48. NATO. NATO Strategic Communications Policy. Brussels : NATO, [б. p.]. URL: https://info.publicintelligence.net/NATO-STRATCOM-Policy.pdf

49. NATO. Riga Summit Declaration. Brussels : NATO, 2006. URL: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2006/11/29/riga-summit-declaration

50. NATO. The Alliance's New Strategic Concept 1991. Brussels : NATO, 1991. URL: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/1991/11/08/the-alliances-new-strategic-concept-1991

51. NATO. Wales Summit Declaration : Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales, 05 September 2014. Brussels : NATO, 2014. URL: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2014/09/05/wales-summit-declaration

52. NATO. Warsaw Summit Communiqué. Brussels : NATO, 2016. URL: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique

53. NATO's Approach to Counter Information Threats : Official text, 18 October 2024. *NATO*. URL:

https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/10/18/natos-approach-to-counter-information-threats

54. NCI Agency Technology Strategy. Brussels : *NATO Communications and Information Agency*, [б. p.]. URL: https://www.ncia.nato.int/resources/site1/General/newsroom/publications/Public_NCIA_Technology%20Strategy_external_v6%20-%20digital.pdf

55. One Year of JATEC: Strengthening Ukraine–NATO Cooperation and Innovation. *The Odessa Journal*. 2025. URL: https://odessa-journal.com/one-year-of-jatec-strengthening-ukraine-nato-cooperation-and-innovation

56. Resilience, Civil Preparedness and Article 3. *NATO*. 13 November 2024. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3

57. RESIST 3: Building Resilience to Information Threats. *UK Government Communications Service.* URL: https://www.communications.gov.uk/publications/resist-3-building-resilience-to-information-threats/

58. Russian Cyber Operations Against Ukraine : Declaration by the High Representative on Behalf of the European Union, 10 May 2022. *Council of the European Union.* URL: https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

59. Šenk M., Hynek N. NATO/EU Synergies Against Information Warfare: A "Circulatory Institutionalist" Model of Expert Voluntarism. *European Security.* 2025. DOI: 10.1080/09662839.2025.2566519

60. Setting the Record Straight. *NATO*. URL: https://www.nato.int/en/what-we-do/wider-activities/natos-approach-to-counter-information-threats/setting-the-record-straight

61. Shaping the Future of Strategic Communications in NATO. *NATO ACT*. 2025. URL: https://www.act.nato.int/article/stratcom-coe-2025/

62. Strategic Communication: A Caution to Military Commanders. *Military Review.* 2017. November. URL: https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2017-Online-Exclusive-Articles/Strategic-Communication/

63. The Cognitive Battlefield of Hybrid Warfare. *NATO Defense College Foundation.* URL: https://www.natofoundation.org/food/the-cognitive-battlefield-of-hybrid-warfare/

64. The Secretary General's Annual Report 2023. Brussels : *NATO*, 2024. URL: https://www.nato.int/content/dam/nato/legacy-wcm/media_pdf/2024/3/pdf/sgar23-en.pdf

65. The Secretary General's Annual Report 2024. Brussels : *NATO,* 2025. URL: https://www.nato.int/content/dam/nato/legacy-wcm/media_pdf/2025/4/pdf/sgar24-en.pdf

66. UK Ministry of Defence. AJP-10 Allied Joint Doctrine for Strategic Communications. Change 1. London : UK MoD, 2023. URL: https://assets.publishing.service.gov.uk/media/6525459d244f8e00138e7343/AJP_10_Strat_Comm_Change_1_web.pdf

67. United Nations General Assembly. Resolution 78/237. New York : *UN*, 2023. URL: https://docs.un.org/en/a/res/78/237

68. United Nations. Our Common Agenda : Policy Brief — Information Integrity on Digital Platforms. New York : *UN*, 2023. URL: https://brasil.un.org/sites/default/files/2023-06/our-common-agenda-policy-brief-information-integrity-en.pdf

69. War Speeches, Negotiations, War with NATO and the Absence of Ukraine: What Did Russia Lie About in January? *Opora Ukraine,* 01 лютого, 2024. URL:

https://oporaua.org/en/viyna/war-speeches-negotiations-war-with-nato-and-the-absence-of-ukraine-what-did-russia-lie-about-in-january-25092

70. WE ARE NATO: Defence and Security Campaign Toolkit. Brussels : *NATO ACT*, 2023. URL: https://www.act.nato.int/wp-content/uploads/2023/06/nato-dsct.pdf

71. What is NATO's Approach to Counter Information Threats? : інформаційний листок. Brussels : NATO, 2024. URL: https://www.nato.int/content/dam/nato/legacy-wcm/media_pdf/2024/12/pdf/2412-Information-Threats.pdf