Євгенія ЛУК'ЯНЧЕНКО
ORCID: 0000-0002-3586-1228

ЕВОЛЮЦІЯ ПОЛІТИКИ НАТО ЩОДО ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ (2014-2021)

DOI: 10.15330/apiclu.69.4.40-4.52

Постановка проблеми. Російська агресія проти України у 2014 році, що розпочалася з незаконної анексії Криму та збройного конфлікту на сході України, супроводжувалася масштабними та скоординованими кампаніями дезінформації. Інформаційні операції стали невід'ємною складовою гібридної війни, спрямованої на підрив довіри до демократичних інституцій, дестабілізацію суспільств і послаблення єдності Північноатлантичного альянсу. За цих умов постала потреба у системній, узгодженій та довгостроковій політиці НАТО щодо протидії інформаційним загрозам, що й зумовлює актуальність даного дослідження.

Аналіз останніх досліджень і публікацій. Проблематика протидії дезінформації у політиці НАТО активно досліджується як у межах офіційних документів Альянсу, так і в аналітичних матеріалах НАТО Парламентської асамблеї та експертних центрів. Зокрема, на офіційному сайті НАТО системно висвітлюється підхід Альянсу до протидії інформаційним загрозам та гібридним впливам [1; 3]. Важливе значення мають матеріали серії Setting the Record Straight, присвячені спростуванню російської дезінформації [2]. Аналітичні доповіді НАТО ПА (Р. Демеуз, Ж. Гарріо Майлам) розкривають стратегічний вимір «війни за правду», яку веде Росія проти демократичних держав [5; 6]. Українські дослідники також аналізують роль НАТО у зміцненні інформаційної стійкості України та перспективи співпраці у цій сфері [8; 9]. Водночас еволюція політики НАТО саме у період 2014–2021 років потребує цілісного узагальнення, що й становить наукову нішу цієї статті.

Формулювання цілей статті. Метою статті є комплексний аналіз еволюції політики НАТО щодо протидії дезінформації у 2014–2021 роках, визначення ключових етапів, інструментів та

ініціатив Альянсу, а також оцінка їх значення для формування сучасної системи інформаційної безпеки НАТО і його партнерів.

Виклад основного матеріалу. Масштабні інформаційні атаки, що супроводжували перші етапи російсько-української війни (анексію Криму і бойові дії на сході України), стали тривожним сигналом для НАТО. Альянс оперативно відреагував на цей виклик: вже в січні 2014 року було відкрито Центр передового досвіду НАТО з питань стратегічних комунікацій («StratCom COE») у Ризі на основі меморандуму, підписаного сьома державами–членами (країни Балтії, Польща, Велика Британія, Німеччина та Італія). «StratCom COE» став майданчиком для вивчення природи інформаційних загроз, напрацювання методів протидії та підготовки експертів. У наступні роки до роботи центру долучалися нові країни: у 2016 році – Нідерланди і Фінляндія, 2017 – Швеція, 2018 – Канада, 2019 – Словаччина, 2020 – США та Данія, а 2021 – Франція і Угорщина. Широке коло учасників відображало усвідомлення спільної загрози і потребу координувати зусилля.

Вже у 2015 році НАТО ухвалило першу Стратегію щодо протидії гібридній війні, яка окреслювала роль Альянсу у боротьбі з комбінацією військових та невійськових загроз, включно з кібератаками та дезінформацією. Поступово у доктринах НАТО закріпилося сучасне розуміння «гібридних загроз» – скоординованого використання різних засобів (військових, кібернетичних, економічних, інформаційних тощо) для досягнення агресором цілей без відкритої війни. Дезінформація розглядається як ключовий елемент гібридної тактики: вона покликана розмивати межу між війною та миром і підривати стійкість держав із середини. У зв'язку з розмиттям поняття «дезінформація» в публічному дискурсі, НАТО ввело ширший термін «інформаційні загрози», що охоплює весь спектр ворожих інформаційних впливів – від цілеспрямованого поширення фейків до прихованого втручання зовнішніх акторів у інформаційне середовище. Водночас НАТО наголошує, що його підхід не передбачає цензуру чи обмеження свободи слова – Альянс протидіє зовнішнім інформаційним операціям, поважаючи свободу вираження поглядів.

Важливим кроком стало офіційне визнання, що ворожі інформаційні операції можуть трактуватися як достатньо серйоз-

на загроза безпеці, щоб за певних обставин стати підставою для колективної оборони. З 2016 року союзники публічно заявляли, що масштабні гібридні дії проти однієї чи кількох країн НАТО можуть призвести до рішення про застосування статті 5 Вашингтонського договору про колективну оборону.

Протягом 2014–2021 років НАТО послідовно розбудовувало механізми протидії інформаційним загрозам. Було вдосконалено систему стратегічних комунікацій: створено посади та підрозділи, відповідальні за «StratCom» (стратегічні комунікації) як на рівні штаб-квартири, так і в командних структурах. У 2018 році на саміті в Брюсселі лідери НАТО ухвалили рішення сформувати групи підтримки з протидії гібридним загрозам («Counter-Hybrid Support Teams»), що на запит країни-союзниці надаватимуть їй цільову експертну допомогу в підготовці до відбиття гібридних атак. Уже в листопаді 2019 року перша така команда була розгорнута в Чорногорії для посилення її спроможностей протидіяти діям Росії. Цей випадок став показовим, адже Чорногорія зазнавала інтенсивної пропагандистської атаки під час вступу до НАТО. Пізніше подібну команду залучали й для допомоги Литві у 2021 році. Такі місії дали змогу напрацювати модель швидкого реагування на інформаційні кризи в окремих країнах.

Паралельно НАТО зміцнювало співпрацю з Європейським Союзом та окремими партнерами. У 2016 році було започатковано обмін інформацією між Аналітичним відділом з гібридних загроз НАТО та Гібридною розвід-групою ЄС, аби покращити ситуаційну обізнаність про ворожі інформаційні кампанії. У 2017 році в Гельсінкі відкрився Європейський центр передового досвіду з протидії гібридним загрозам, підтриманий як НАТО, так і ЄС. Він став важливою платформою для спільних досліджень і тренінгів у цій сфері.

У Варшавському комюніке 2016 року особливу увагу приділили Україні: було створено Платформу НАТО–Україна з протидії гібридній війні, покликану обмінюватися досвідом виявлення гібридних загроз і зміцнювати стійкість України. Цей механізм охоплював проєкти з дослідження уроків протистояння російській агресії, програми підготовки та експертні консультації, в тому числі з протидії дезінформації та зміцнення стійкості.

У відповідь на російські наративи, що намагалися представити НАТО «ворожим» або «неспроможним», Альянс активізував публічну дипломатію. У 2017 році НАТО запустило масштабну комунікаційну кампанію «We Are NATO» («Ми — НАТО»), націлену на підвищення обізнаності громадян країн-членів про оборонну роль і цінності Альянсу. Ця ініціатива стала першою настільки широкою за останні десятиліття: у її рамках НАТО за допомогою соціальних мереж, відео та подій демонструвало єдність союзників, їхній внесок у спільну безпеку, тим самим спростовуючи нав'язувані Кремлем міфи про «розкол» чи «занепад» Альянсу. Ще одним напрямом стало нарощування присутності в інформаційному просторі. НАТО значно активізувалося в цифрових медіа, особливо в період пандемії COVID-19. Це дозволило розширити охоплення шляхом переходу на нові платформи та активнішого використання соцмереж. Наприклад, починаючи з 2020 року, офіційні сторінки НАТО та національні центри «StratCom» регулярно публікували факти і спростування дезінформації щодо пандемії та ролі НАТО у протидії їй, оскільки і Росія, і Китай поширювали неправдиві версії про походження вірусу та взаємну допомогу. Цей досвід ще більше переконав Альянс у важливості проактивних комунікацій.

Загалом у період з 2014 по 2022 рік НАТО виробило базові принципи протидії дезінформації. По-перше, Альянс ніколи не відповідає пропагандою на пропаганду, натомість спирається на перевірені факти та достовірні джерела. По-друге, діяти проактивно, доносити власну інформацію та цінності раніше, ніж противник нав'яже свою повістку. По-третє, виваженість і цілеспрямованість у спростуванні фейків: НАТО свідомо не намагається спростувати кожну неправдиву заяву, адже це може посилити їхній резонанс. Замість цього застосовується селективний підхід – відповідають на найбільш небезпечні або широко розповсюджені дезінформаційні наративи, використовуючи чіткі і зрозумілі повідомлення з фактами та цифрами. По-четверте, комплексна побудова стійкості. НАТО прагне сформувати у своїх суспільствах певний «інформаційний імунітет», тобто критичне мислення та несприйнятливість до чужої пропаганди. Це досягається просві-

тою, підтримкою незалежних медіа, розвитком медіаграмотності. По-п'яте, безперервний моніторинг і аналіз інформаційного середовища: збір даних про ворожі кампанії, вивчення їхніх методів і цілей – усе це живить адаптацію комунікаційної стратегії НАТО.

Ключові заходи (2014–2021):

Рік	Політика ініціатива НАТО	Короткий опис та значення
2014	Відкриття «StratCom COE» (Рига)	Засновано Центр передового досвіду НАТО зі стратегічних комунікацій у відповідь на інформаційні атаки Росії. У липні 2014 сім країн підписали угоду про діяльність центру.
2015	Стратегія НАТО щодо гібридної війни	Альянс ухвалив першу стратегію протидії гібридним загрозам, що включала боротьбу з ворожою пропагандою і кібератаками.
2016	Варшавський саміт – визнання гібридних загроз	Оголошено, що значні гібридні дії (в т.ч. дезінформація) можуть спричинити застосування ст. 5 НАТО. Створено Платформу НАТО–Україна з протидії гібридній війні для обміну досвідом у боротьбі з дезінформацією.
2017	Кампанія «We Are NATO»	НАТО розпочало широкомасштабну публічну кампанію для зміцнення підтримки Альянсу та спростування міфів про нього. Також відкрито Європейський Центр протидії гібридним загрозам (Гельсінкі) за участі НАТО і ЄС.
2018	Брюссельський саміт – підтримка для союзників	Лідери НАТО домовилися створити команди протидії гібридним загрозам, що надають допомогу країнам-членам на їхній запит у разі гібридної атаки.
2019	Перший виїзд експертної команди	НАТО вперше розгорнуло команду з протидії гібридним загрозам у Чорногорії, щоб допомогти нейтралізувати російські дезінформаційні й інші підривні акції проти цієї країни.
2020	Цифровізація комунікацій	НАТО посилило роботу в онлайн-просторі через пандемію COVID-19, розширило аудиторію та активно спростовувало дезінформацію щодо COVID-19 та діяльності НАТО під час кризи.
2021	Стратегічний діалог і навчання	Проведено перший Київський форум зі стратегічних комунікацій за участі НАТО, ЄС та України. НАТО «StratCom COE» реалізував низку проєктів: розробку доктрини, тренінги з контрдезінформації, аналіз контрнаративів тощо. НАТО-Україна спільно навчали фахівців зі стратегічних комунікацій і обмінювалися досвідом протидії російським інформаційним операціям.

Новий етап: протидія дезінформації після 2022 року

Повномасштабне вторгнення Росії в Україну у лютому 2022 року ознаменувало безпрецедентне загострення інформаційної війни. Кремль розгорнув глобальну кампанію брехні, щоб виправдати агресію та зламати міжнародну підтримку України. У відповідь НАТО суттєво активізувало зусилля з викриття та нейтралізації цієї дезінформації.

На Мадридському саміті в червні 2022 року союзники ухвалили нову Стратегічну концепцію НАТО, в якій прямо вказали, що Росія становить «найбільш значну і пряму загрозу» безпеці євроатлантичного регіону, використовуючи проти союзників та партнерів у тому числі методи гібридної війни і дезінформацію. Одночасно відзначено й виклики з боку Китаю: агресивна риторика Пекіна та кампанії дезінформації підривають безпеку, зокрема через поширення маніпулятивних наративів і політичний вплив. Усвідомлюючи нову реальність, лідери НАТО в липні 2022 року схвалили комплексні заходи запобігання та реагування на гібридні загрози, що можуть гнучко застосовуватися залежно від ситуації.

Від початку вторгнення НАТО не залишало без відповіді жодної гучної дезінформаційної атаки Москви. Генеральний секретар і представники Альянсу регулярно виступали із заявами, де надавали факти та спростування. Зокрема, вже у березні 2022 року НАТО публічно наголошувало, що не є стороною конфлікту в Україні і не прагне конфронтації з Росією, на противагу кремлівськиій пропаганді про «НАТО у війні проти Росії». НАТО почало систематично викривати найпоширеніші фейки Москви про Альянс і війну. Наприклад, на офіційному сайті НАТО створено спеціальний розділ «Setting the Record Straight» («Розставляємо крапки над ‘і’»), де регулярно спростовуються основні російські дезінформаційні тези щодо НАТО. Важливо, що НАТО подає лише перевірені факти й посилання на авторитетні джерела, дотримуючись своєї принципової лінії – боротися з дезінформацією правдою, а не контрпропагандою.

НАТО також координувало інформаційну діяльність союзників: країни-члени обмінювалися даними про російську дезінфор-

мацію, ділилися перекладами та аргументами для спростування. За підтримки НАТО та ЄС у 2022–2023 роках було створено низку міжнародних оперативних груп з протидії дезінформації, які відстежували ключові наративи Кремля і виробляли спільні відповіді. Одночасно Альянс зміцнив внутрішню стійкість: країни-члени отримали оновлені рекомендації щодо захисту власного інформаційного простору, забезпечення кібербезпеки телекомунікацій та реагування на спроби зовнішнього втручання у демократичні процеси (як-от вибори). У 2023 році на саміті у Вільнюсі лідери НАТО підтвердили непохитність підтримки України і водночас оголосили про нові кроки зі зміцнення стійкості союзників – від захисту критичної інфраструктури до боротьби з іноземною інформаційною маніпуляцією. Комюніке саміту окремо відзначило необхідність протидіяти дезінформаційній діяльності з боку КНР та інших авторитарних акторів, глобалізуючи цим самим підхід НАТО до інформаційних загроз.

З початком повномасштабної війни **НАТО безпрецедентно активізувало допомогу Україні** не лише у військовій чи політичній площині, а й в інформаційній. Уже в березні 2022 року відбулися термінові консультації НАТО–Україна на рівні Комісії, де обговорювали в тому числі інформаційну складову агресії. У липні 2023 року цю Комісію було трансформовано в повноцінну Раду НАТО–Україна, надавши Києву більше можливостей прямо брати участь у плануванні спільних дій і обміні розвідданими щодо гібридних загроз.

Однією з ключових платформ залишається згадана Платформа з протидії гібридній війні, яка після 24 лютого 2022 року переорієнтувалася на нагальні потреби: вона підтримує дослідження уроків війни Росії проти України, проводить тренінги з протидії дезінформації та консультує українські органи щодо зміцнення стійкості суспільства. Крім того, у 2022-му розширено Комплексний пакет допомоги (CAP) для України – туди включено заходи з посилення довгострокової стійкості, зокрема в інформаційній сфері. У межах CAP та інших програм НАТО фінансувало проєкти з навчання українських фахівців стратегічних комунікацій, зміцнення кіберзахисту медійної інфраструктури, протидії кібератакам на телебачення та урядові сайти тощо.

Дуже важливим напрямом стала просвітницька та тренінгова підтримка. НАТО сприяло численним навчанням з медіаграмотності й протидії дезінформації для українських держслужбовців, військових та представників громадянського суспільства. За останні два роки в Україні проведено понад 200 тренінгів із протидії дезінформації, які пройшли більше 2000 осіб із органів влади – багато з цих заходів відбулися за методичної чи експертної участі фахівців НАТО. У вересні 2025 року в Україні стартувала нова освітня програма для місцевих громад з виявлення і нейтралізації російських інформаційних маніпуляцій – проєкт було підготовлено громадською організацією за підтримки Офісу НАТО в Україні та Центру протидії дезінформації РНБО. Представниця НАТО Вінета Кляйне наголосила, що здатність громад протистояти маніпуляціям – важливий елемент загальної стійкості суспільства. За її словами, «наративи, засновані на демократичних цінностях, успішно протидіють маніпулятивним наративам Росії», і НАТО навчається в України, як ефективно боротися з дезінформацією.

Не менш активно НАТО координує зусилля з Європейським Союзом у протидії кремлівській пропаганді щодо війни. ЄС ще з 2015 року веде проєкт «EUvsDisinfo», і з 2022 року аналітики НАТО та ЄС регулярно обмінюються трендами дезінформації та узгоджують основні меседжі протидії. НАТО залучилося до користування системою «Rapid Alert System» ЄС для раннього попередження про інформаційні операції, що дозволило союзникам швидше дізнаватися про нові фейки та спільно виробляти стратегії реагування. Крім того, НАТО і ЄС провели серію паралельних навчань з гібридних загроз, в рамках яких опрацьовували і сценарії масових кампаній дезінформації та спільні дії у відповідь.

Механізми НАТО: моніторинг, реагування, стратегічні комунікації і навчання

НАТО вибудувало багаторівневу систему протидії інформаційним атакам, яка включає як розвідувально-аналітичні елементи, так і інструменти публічної дипломатії та підготовки кадрів.

У структурі Штаб-квартири НАТО діє Об'єднаний розвідувально-безпековий підрозділ (JISD), в якому ще у 2017 році створено окремий «Hybrid Analysis Branch» – аналітичний відділ з

протидії гібридним загрозам. Його завдання – цілодобово відстежувати інформаційне середовище, виявляти ознаки координації інформаційних атак, аналізувати джерела та націленість ворожих наративів. Ця інформація у режимі реального часу доводиться до вищого керівництва НАТО, дозволяючи приймати рішення оперативно. Паралельно працюють і національні структури – розвідки держав-союзниць, які діляться своїми даними про впливові інформаційні операції. Для полегшення обміну була налагоджена пряма комунікація між згаданим відділом НАТО та «Hybrid Fusion Cell» ЄС (аналогічним аналітичним осередком Європейської служби зовнішніх дій). Спільні наради та відеоконференції між аналітиками НАТО, ЄС та експертами Гельсінського Центру передового досвіду стали регулярними і дозволяють напрацьовувати спільну ситуаційну картину інформаційних загроз. Хоча обмін чутливою (секретною) розвідувальною інформацією має обмеження, сторони максимально використовують відкриті джерела та спільні оцінки, щоб не пропустити небезпечних тенденцій.

Коли ідентифіковано конкретну дезінформаційну атаку, НАТО застосовує комбінацію інструментів для реагування, як негайних, так і довгострокових. На короткостроковому рівні працюють команди швидкого інформаційного реагування: пресслужба НАТО та національні представники (спікери) узгоджують основні меседжі й дають публічні спростування або коментарі. Часто НАТО залучає і незалежних експертів, і відомих особистостей для посилення достовірності повідомлень. Наприклад, аби нейтралізувати російську дезінформацію про «біолабораторії США в Україні», НАТО співпрацювало з ООН, ЄС та авторитетними вченими, які надали детальні роз'яснення, що жодної біологічної зброї не розроблялося. Одночасно, в НАТО рішення, чи реагувати публічно на кожен інформаційний привід, ухвалюється зважено: береться до уваги потенційна шкода від дезінформації та її охоплення.

На середньостроковому рівні НАТО вживає заходів для запобігання повторенню успішних інформаційних атак. Сюди входить тісна взаємодія з урядами держав-членів: аналізуючи конкретний

випадок дезінформації, НАТО допомагає виявити «вразливі місця» – аудиторії чи теми, на які ворог націлився, – і рекомендує, як їх укріпити. Іншим компонентом є обмін досвідом між країнами: ті держави НАТО, що мали справу з певною тактикою дезінформації, діляться своїми уроками і найкращими практиками реагування з іншими союзниками. Такий обмін координується через Центри передового досвіду, які організовують семінари і видають аналітичні звіти для урядовців.

На довгостроковому рівні НАТО інвестує у підвищення загальної стійкості суспільств до інформаційних загроз. Ще в 2016 році на Варшавському саміті країни НАТО затвердили 7 базових вимог до національної стійкості, одна з яких – забезпечення стійких систем комунікації та здатності суспільства протистояти дезінформації. Відтоді кожна держава регулярно звітує про виконання цих вимог, а НАТО надає методичну допомогу. Стратегічні комунікації включено до програм підготовки офіцерів та цивільних кадрів НАТО. У Військовому коледжі НАТО та Школі НАТО проводяться курси з інформаційної безпеки, роботи з громадськістю в умовах гібридних впливів тощо. Проводяться й спільні навчання: наприклад, навчання спецпризначенців «Nighthawk 21» у 2021 році включало сценарії протидії тероризму та елементам гібридної війни, де учасники відпрацьовували й реагування на кампанії ворожої пропаганди. Таким чином формується культура врахування інформаційного виміру в усіх операціях НАТО.

Робота з партнерами також є важливим механізмом. Окрім України, НАТО допомагає зміцнювати інформаційну стійкість Грузії, Молдови, країн Балканського регіону. На прохання урядів можуть надсилатися консультативні групи з питань стійкості (RAST) – такі місії працювали в Україні у 2019–2022 роках, готуючи рекомендації для захисту критичної інфраструктури та цивільного населення від гібридних загроз. Прямо з дезінформацією ці групи не борються, але їхні поради щодо кризових комунікацій, захисту енергомереж чи кібербезпеки допомагають унеможливити ряд інформаційно-психологічних операцій ворога. Крім того, НАТО активно залучає партнерів до своїх програм у сфері «StratCom». Так, представники України, Грузії, а також до

їхнього вступу, Фінляндії та Швеції, щорічно запрошувались на Конференцію комунікаторів НАТО, де зустрічаються прес-секретарі та фахівці зі зв'язків з громадськістю всіх держав Альянсу.

Зрештою, НАТО робить ставку на інновації. Розуміючи, що противник використовує нові технології – від ботів у соцмережах до штучного інтелекту для генерування фейкових зображень і відео. Відтак, Альянс підтримує дослідження в цій сфері. У «StratCom COE» в Ризі діє експериментальна лабораторія, де вивчають можливості штучного інтелекту у виявленні та протидії дезінформації. Також НАТО фінансує проєкти через програму Наука заради миру і безпеки (SPS), спрямовані на створення інструментів автоматичного моніторингу соцмереж, аналізу великих даних для виявлення координованих інформаційних атак та навіть систем, що дозволяють відстежувати походження дезінформації. Це довгострокові ініціативи, вони мають на меті дати Альянсу технологічну перевагу у «битві алгоритмів» майбутнього.

Висновок. Еволюція політики НАТО щодо протидії дезінформації у 2014–2021 роках засвідчує трансформацію підходів Альянсу до сучасних безпекових викликів. Від усвідомлення загрози до створення спеціалізованих інституцій, нормативних рамок і практичних механізмів НАТО поступово сформувало цілісну систему протидії інформаційним загрозам. Ця система ґрунтується на принципах правдивості, проактивності, селективного реагування та зміцнення стійкості суспільств. Події після 2022 року підтвердили актуальність напрацьованих підходів і водночас засвідчили необхідність їх подальшого розвитку в умовах глобалізації інформаційних конфліктів.

1. NATO's approach to counter information threats : NATO Official Website. Updated 2025. 03 Feb. URL: https://www.nato.int

2. Setting the Record Straight – De-bunking Russian disinformation on NATO : NATO Official Website. Updated 2025. 06 Nov. URL: https://www.nato.int

3. Countering hybrid threats : NATO Official Website. Updated 2024. 07 May. URL: https://www.nato.int

4. Relations with Ukraine – Response to Russia's war against Ukraine : NATO Official Website. Updated 2023. 27 Oct. URL: https://www.nato.int

5. *Demeuse R. Russian War on Truth: Defending Allied and Partner Democracies against the Kremlin's Disinformation Campaigns : General Report. NATO Parliamentary Assembly. 2023. 08 Oct. URL: https://www.nato-pa.int*
6. *Garriaud-Maylam J. The Russian War on Truth : Report. NATO PA. 2023. URL: https://www.nato-pa.int*
7. *NATO Assembly calls for decisive action on cyberattacks and disinformation, stronger partnerships : News Article. NATO PA. 2025. 25 May. URL: https://www.nato-pa.int*
8. *Цехановська О. НАТО проти дезінформації: як Україна може розвивати співпрацю з Альянсом. Рада зовнішньої політики «Українська призма». 2021. 15 листоп. URL: http://prismua.org*
9. *У НАТО радять дозовано підходити до спростування дезінформації : новина. Укрінформ. 2021. 07 груд. URL: https://www.ukrinform.ua*
10. *Відповідь на сучасні загрози: в Україні запускають курс для громад з протидії російським маніпуляціям : новина. Media Center Ukraine. 2025. 05 верес. URL: https://mediacenter.org.ua*

Лук'янченко Євгенія. Еволюція політики НАТО щодо протидії дезінформації (2014-2021)

У статті проаналізовано еволюцію політики НАТО щодо протидії дезінформації в період 2014–2021 років. Протягом 2014–2021 років НАТО послідовно розбудовувало механізми протидії інформаційним загрозам. Було вдосконалено систему стратегічних комунікацій: створено посади та підрозділи, відповідальні за «StratCom» (стратегічні комунікації) як на рівні штаб-квартири, так і в командних структурах. У 2018 році на саміті в Брюсселі лідери НАТО ухвалили рішення сформувати групи підтримки з протидії гібридним загрозам («Counter-Hybrid Support Teams»), що на запит країни-союзниці надаватимуть їй цільову експертну допомогу в підготовці до відбиття гібридних атак. Уже в листопаді 2019 року перша така команда була розгорнута в Чорногорії для посилення її спроможностей протидіяти діям Росії. Цей випадок став показовим, адже Чорногорія зазнавала інтенсивної пропагандистської атаки під час вступу до НАТО. Пізніше подібну команду залучали й для допомоги Литві у 2021 році. Такі місії дали змогу напрацювати модель швидкого реагування на інформаційні кризи в окремих країнах.

Досліджено передумови формування відповідних механізмів Альянсу у відповідь на зростання інформаційних загроз, пов'язаних насамперед із російською агресією проти України. Визначено ключові інституційні, нормативні та практичні заходи НАТО у сфері стратегічних комунікацій і протидії гібридним загрозам, а також їх значення для безпеки союзників і партнерів. Окрему увагу приділено новому етапу політики НАТО з протидії дезінформації після 2022 року.

Ключові слова: дезінформація, гібридні загрози, НАТО, стратегічні комунікації, інформаційна безпека.

Ievgeniia Lukianchenko. The evolution of NATO's policy on countering disinformation (2014-2021)

The article analyzes the evolution of NATO's policy on countering disinformation in the period 2014–2021. During 2014–2021, NATO consistently developed mechanisms for countering information threats. The strategic communications system was improved: positions and units responsible for «StratCom» (strategic communications) were created both at the headquarters level and in command structures. In 2018, at the Brussels summit, NATO leaders decided to form Counter-Hybrid Support Teams, which, at the request of allied countries, will provide it with targeted expert assistance in preparing to repel hybrid attacks. Already in November 2019, the first such team was deployed in Montenegro to strengthen its capabilities to counter Russia's actions. This case became indicative, as Montenegro was subjected to an intense propaganda attack during its accession to NATO. Later, a similar team was also involved to assist Lithuania in 2021. Such missions made it possible to develop a model of rapid response to information crises in individual countries.

The prerequisites for the formation of appropriate Alliance mechanisms in response to the growth of information threats, primarily related to Russian aggression against Ukraine, were studied. NATO's key institutional, regulatory and practical measures in the field of strategic communications and countering hybrid threats were identified, as well as their significance for the security of allies and partners. Special attention is paid to the new stage of NATO's policy on countering disinformation after 2022.

Keywords: disinformation, hybrid threats, NATO, strategic communications, information security.