МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ МІЖНАРОДНИХ ВІДНОСИН
КАФЕДРА МІЖНАРОДНИХ ВІДНОСИН, ІНФОРМАЦІЇ ТА РЕГІОНАЛЬНИХ СТУДІЙ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____ Ніна РЖЕВСЬКА
«_15_» _____06_____ 2023р.

**КВАЛІФІКАЦІЙНА РОБОТА**
ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА
СПЕЦІАЛЬНІСТІ 291 «МІЖНАРОДНІ ВІДНОСИНИ, СУСПІЛЬНІ КОМУНІКАЦІЇ ТА РЕГІОНАЛЬНІ СТУДІЇ»
ОСВІТНЬО-ПРОГРАМНОЇ ПРОГРАМИ
«МІЖНАРОДНА ІНФОРМАЦІЯ»

**Тема**: **«СТРАТЕГІЧНІ КОМУНІКАЦІЇ НАТО ЯК СКЛАДОВА ЗОВНІШНЬОПОЛІТИЧНОЇ ДІЯЛЬНОСТІ АЛЬЯНСУ»**

Виконавець: здобувач вищої освіти 4 курсу, 409 група, Щава Кристина Олександрівна

Керівник: к.і.н., доцент кафедри міжнародних відносин, інформації та регіональних студій Боротканич Наталія Петрівна

Нормоконтролер: _____ Олексій МЕНДРІН
(підпис)

КИЇВ 2023

**ЗМІСТ**

# ВСТУП

**Актуальність теми дослідження** полягає в тому, що під час холодної війни політика НАТО щодо оборони та стримування зосереджувалася переважно на жорсткій силі. У цей час інформаційна політика відігравала додаткову і здебільшого непомітну роль, оскільки стримування базувалося головним чином на розробці та розгортанні систем озброєнь і військових підрозділів на території НАТО, особливо в Європі. Інформаційна війна була сформована в основному традиційними засобами масової інформації, керованими державами, і обидві сторони, НАТО та Варшавський договір, прагнули інформувати власне населення, а не впливати на іншу сторону.

Проте швидкий розвиток інформаційних технологій і посилення ролі ЗМІ в епоху після холодної війни змінили важливість інформаційних воєн. Зміна характеру операцій після закінчення Холодної війни, які посилюють увагу до прав людини, також підвищила важливість публічної інформації і системи стратегічних комунікацій. Громадськість також стала більш чутливою до дезінформації та пропаганди, і інформаційна війна стала майже рівноцінною традиційній війні.

Таким чином, нові місії та операції Альянсу, такі як у Боснії, Косово чи Афганістані, були зосереджені на підтримці та розбудові миру, а не на конфліктах, і це підвищило важливість зв’язків із громадськістю та діяльності ЗМІ в Альянсі. Однак брак досвіду НАТО в цій сфері призвів до того, що його сили не змогли заручитися громадською підтримкою в цих нових місіях, а також підкреслив обмеження традиційних військових операцій. Ця невдача змусила Альянс зосередитися на громадській дипломатії та діяльності StratCom, що є відносно новим і мало вивченим аспектом діяльності Альянсу.

Актуальність теми також підкріплюється ще й тим фактом, що сьогодні гібридна війна стала основною формою ведення воєн і вийшла на перший план, обійшовши навіть фізичні бойові дії. Саме тому НАТО дуже важливо розвивати сектор стратегічних комунікацій, щоб Альянс міг ефективно давати відсіч

дезінформації і фейковим новинам, а також міг інформувати своїх громадян і сповіщати їх про реальну ситуацію.

Найбільш важливими в науковому розумінні для автора під час написання кваліфікаційної роботи були праці таких вчених, як Д. Любарець, У.Ільницької, А.Олійник, О.Рітмана, Д. Рейдінга, Б.Велса, М.Митровича, М.Фроста, С.Растона, які досліджували проблематику стратегічних комунікацій, особливостей їх використання в умовах сучасної політичної дійсності і деякі аспекти практичної реалізації стратегічних комунікацій в діяльності НАТО.

**Метою кваліфікаційної роботи** є дослідження ролі системи стратегічних комунікацій НАТО як складової зовнішньополітичної діяльності Альянсу.

Відповідно до поставленої мети визначено **основні завдання**:

– вивчити поняття, принципи та вектори реалізації комунікативних стратегій НАТО;

– розглянути історію становлення та трансформації інституту стратегічних комунікацій Північноатлантичного Альянсу;

– описати інституційний та нормативно-правовий вимір реалізації інформаційно-комунікативної політики організації;

– механізми та засоби практичного здійснення стратегічних комунікацій Північноатлантичного Альянсу;

– провести аналіз стратегічних комунікацій НАТО як дієвого механізму протидії дезінформації і гібридним війнам;

– визначити нові підходи Північноатлантичного Альянсу у сфері кібербезпеки в умовах загострення інформаційного протистояння;

– проаналізувати діджиталізацію процесів публічної комунікації як одного із пріоритетних напрямків інформаційної політики НАТО;

– дослідити стан і перспективи інформаційної діяльності НАТО щодо євроатлантичної інтеграції України.

**Об’єктом дослідження** є Центр стратегічних комунікацій Stratcom НАТО як один із пріоритетних підрозділів Альянсу в умовах сучасних викликів.

**Предметом дослідження** є механізми та засоби здійснення процесу стратегічних комунікацій НАТО.

**Методологія дослідження.** Теоретико-методологічну основу кваліфікаційної роботи становлять наукові праці вітчизняних і зарубіжних учених та спеціалістів, матеріали міжнародних і вітчизняних періодичних видань, установчі документи організації, періодичні видання Альянсу і офіційні веб-сайти НАТО.

Для досягнення поставленої мети в дипломній роботі застосовані як загальнонаукові, так і спеціальні методи дослідження.

В першому розділі роботи застосовувався історичний метод для вивчення історії становлення та трансформації інституту стратегічних комунікацій Північноатлантичного Альянсу; діалектичний метод використовувався для розкриття поняття, принципів та векторів реалізації комунікативних стратегій НАТО. Також використовувались методи від абстрактного до конкретного, поєднання аналізу та синтезу, структурно-системного підходу, причиннонаслідкових зв'язків.

В другому розділі роботи використовувались методи контент- та івент-аналізу для розгляду механізмів та засобів практичного здійснення стратегічних комунікацій Північноатлантичного Альянсу.

В третьому розділі використовувався метод моделювання для дослідження перпективних напрямків діяльності Альянсу в системі міжнародних відносин у часи глобальних змін; метод історичного і логічного для вивчення стану і перспектив інформаційної діяльності НАТО щодо євроатлантичної інтеграції України; а також методи причинно-наслідкових, логічних та функціональних зв'язків і залежностей.

Окремі положення роботи пройшли апробацію на XXIII Міжнародній науково-практичній конференції здобувачів вищої освіти і молодих вчених «Політ-2023», XVI Міжнародній науково-технічій конференції «АВІА-2023» та Всеукраїнській науково-практичній конференції з міжнародною участю «Дипломатія в міжнародних відносинах: ретроспекція і сучасність» за матеріалами яких надруковано тези за наступними темами: «Стратегічня комунікаційна діяльність НАТО у відповідь на вторгнення Росії на територію україни», «Наслідки

російсько-української війни для НАТО» та «Механізми публічної дипломатії НАТО» відповідно.

**Структурно** кваліфікаційна робота складається зі вступу, трьох розділів, кожен з яких поділяється на підрозділи, висновків і списку використаних джерел. Обсяг сторінок роботи – 69. Загальний обсяг джерел, які цитуються та є присутніми в списку використаних джерел – 55.

# РОЗДІЛ 1
# КОНЦЕПТУАЛЬНО-ТЕОРЕТИЧНІ ЗАСАДИ РОЗВИТКУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ НАТО

## 1.1.Поняття, принципи та вектори реалізації системи комунікативних стратегій НАТО

Найважливішою тенденцією розвитку сучасного світу слід розглядати глобалізацію. У даному контексті під глобалізацією варто розуміти процес всезростаючого впливу різних факторів міжнародного значення (наприклад, тісних економічних та політичних зв'язків, культурного та інформаційного обміну) на соціальну дійсність в окремих країнах. Її технологічною основою стали інформатизація всіх областей соціальної діяльності, інтеграція інформаційних систем різних держав у єдину загальносвітову інформаційну сферу, формування єдиного інформаційного простору, створення глобальних інформаційно-комунікаційних мереж, інтенсивне впровадження нових інформаційних технологій у всі сфери людської діяльності.

Розвиток інформаційних технологій змінює принципи та методи управління, навчання, він же ліг і в основу революції в галузі міжнародних відносин та у військовій справі.

У цьому контексті одним з найважливіших завдань, які стоять перед сучасними державами, їх військовими відомствами і іншими учасниками і акторами міжнародних відносин, зокрема міжнародні організації, в тому числі НАТО, є використання інформації управління будь-якими конфліктами, оскільки інформація здатна змінювати і впливати на сприйняття людей.

Сьогодні за грамотної стратегії роботи з інформацією можна здобути перемогу в силовому конфлікті. Робота з такими видами інформації, як Інтернет, нові ЗМІ, стала іншим способом ведення сучасних воєн.

Невипадково в США, а потім і в низці інших країн на початку XXI століття відбувається оформлення нового підходу до розгляду ролі масових комунікацій у державній політиці, який одержав своє конкретне втілення у концепції «стратегічна комунікація» [4].

Стратегічна комунікація – це стратегічно скоординована діяльність, спрямована на управління цільовими аудиторіями як усередині країни, так і за її межами з метою підвищення репутації своєї країни або організації на міжнародному рівні, а у разі політичного конфлікту – з метою перемоги в інформаційній війні.

Чинниками швидкого розвитку системи стратегічних комунікацій стали:

– ріст рівня інформатизації суспільства;

– збільшення силових конфліктів у світі;

– підвищення ролі інформаційного протистояння задля досягнення військово-політичних та економічних цілей;

– терористичні атаки;

– формування нових національних стратегій сучасних держав;

– коригування та зміна іміджу країн на міжнародній арені;

– поява та розвиток нових форм дипломатії, таких як громадська дипломатія, кібер-дипломатія [5].

Термін «стратегічна комунікація» у його сучасному розумінні вперше з'явився у військових колах США у 2001 році, проте в офіційних документах США став використовуватись починаючи з 2006 року. Відповідно до чотирирічного плану розвитку, термін «стратегічна комунікація» трактувався як фокусовані зусилля США, спрямовані на розуміння специфіки цільових аудиторій та роботу з ними для створення, зміцнення та збереження урядом США сприятливих умов для просування національних інтересів та цілей шляхом скоординованої інформації, комплексних планів, програм дії та синхронізації з іншими елементами національної влади [6].

Стратегічні комунікації мають зробити вирішальний внесок у розробку та здійснення національної стратегії. Стратегія сприймається як сукупність ідей,

переваг і методів, які пояснюють діяльність (дипломатичну, економічну чи військову) і призводять до поставленої мети. Тому згідно з цією точкою зору, стратегічна комунікація може допомогти зберегти взаємозв'язок між метою та дією.

На даний момент існують і наукові центри для вивчення можливостей стратегічних комунікацій у вирішенні військових конфліктів та запобігання терористичним атакам. Однією з таких організацій є Центр боротьби з тероризмом в Анкарі, створений у 2005 році з метою підтримки НАТО з питань захисту від тероризму. Ще однією науковою організацією, що опікується проблемами стратегічних комунікацій, є Консорціум зі стратегічних комунікацій в Арізонському університеті. Він об'єднує роботу передових учених, викладачів та громадськості у дискусії щодо підвищення ролі комунікації у боротьбі з тероризмом для національної безпеки та у громадській дипломатії.

Сьогодні існує безліч визначень стратегічних комунікацій. Ось деякі з них:

– поєднання двох впливових понять, «м'якої сили» та стримування, які впливають на світову громадську думку;

– безперервний та швидкий потік інформаційних повідомлень, спрямований на цільові аудиторії, який за допомогою сучасних технологічних досягнень та вдалих загальнодержавних методів роботи зі ЗМІ має стати потужним важелем впливу;

– синхронізація слів та справ, і те, як вони будуть сприйняті відібраними аудиторіями; програми та дії, свідомо націлені на спілкування та залучення цільових аудиторій, що здійснюються за допомогою зв'язків з громадськістю, громадської дипломатії та інформаційних операцій [7];

– проектування в масову свідомість державою певних стратегічних цінностей, інтересів та цілей шляхом адекватної синхронізації різнобічної діяльності у всіх сферах суспільного життя з її професійним комунікаційним супроводом [6];

– процес, спрямований на роботу з цільовими аудиторіями щодо створення, зміцнення та збереження сприятливих умов для просування національних інтересів та цілей шляхом скоординованої інформації, комплексних планів, програм дії та синхронізації з іншими елементами національної влади [5];

– систематична серія тривалих і послідовно пов’язаних між собою дій, які проводяться через стратегічні, операційні та тактичні рівні, які дозволяють зрозуміти цільові аудиторії та канали, де може бути просунуто повідомлення для встановлення необхідних типів поведінки цільової аудиторії [8];

– цілий комплекс заходів, вкладених у управління цільовими аудиторіями як у країні, так і за її межами, що складається з трьох частин – зв’язків із громадськістю, громадської дипломатії та інформаційних операцій [7].

Однією з причин такої великої кількості визначень, на думку американського військового аналітика з військового коледжу США Дениса Мерфі, є початкове неточне трактування поняття «стратегічна комунікація» у документах США [9].

Іншою причиною такої величезної кількості визначень стратегічної комунікації є те, що як управлінська дисципліна вона досі перебуває на стадії формування як у теоретичному, так і практичному застосуванні.

Однак, як можна побачити, незважаючи на велику кількість визначень, суть стратегічної комунікації, згідно з усіма трактуваннями, полягає в управлінні цільовими аудиторіями з метою змінити їхню поведінку та донести до них ті цінності чи інформацію, які необхідні державі, що їх застосовує.

Діяльність стратегічної комунікації спрямована не тільки на вплив на певну цільову аудиторію з метою перемоги в інформаційно-психологічній війні, але й на те, щоб поправити імідж країни, що використовує стратегічні комунікації, як у противників, так і союзників за допомогою таких технологій, як іміджмейкінг, брендинг, міжкультурна комунікація, репутаційний менеджмент, спін-лікар.

Важливим завданням, що стоїть перед сучасними міжнародними акторами, серед яких і міжнародні організації, що розробляють практики стратегічних комунікацій, є вміння працювати з її каналами, які останніми роками розширилися завдяки розвитку Інтернет-технологій.

Крім традиційних ЗМІ, експертам, які працюють у галузі стратегічних комунікацій, доводиться освоювати електронні комунікації, які надають нові можливості передачі повідомлення цільовим аудиторіям для розширення ефективної

комунікаційної стратегії, що відповідає за просування державних інтересів та цілей як за кордоном, так і у своїх країнах.

Як зазначають провідні фахівці, старі канали стратегічних комунікацій, наприклад традиційні ЗМІ, були засновані лише на монологічній базі, внаслідок чого аудиторії були лише пасивними споживачами повідомлень.

Поява «нових медіа» відкрила широкі можливості для розвитку діалогічного зв'язку між особами, зацікавленими у посланні повідомлення, та цільовою аудиторією, якій адресовано те чи інше повідомлення. Таким чином, відбувається рівнозначне виробництво та споживання цього повідомлення. За допомогою «нових медіа» комунікатор тепер бачить свою аудиторію, може краще і швидше вибудовувати, коригувати свої повідомлення в залежності від ситуації, що склалася, і настроїв обраної аудиторії, тобто він може керувати її поведінкою.

Фахівці, зайняті в розробках стратегічних комунікацій, виділяють такі електронні канали, з якими в першу чергу потрібно навчитися працювати: електронні ЗМІ (сюди входять журнали, газети, інформаційні агенції), соціальні мережі (найкращими є такі мережі, як Facebook, Twitter), блоги, мобільний зв'язок.

Як зазначалося вище, ЗМІ в Інтернеті мають серйозні переваги перед традиційними ЗМІ. Насамперед, це низька вартість інформаційного продукту; нефіксований обсяг, не обмежений газетними шпальтами або ефірним часом; екстериторіальність, тобто матеріал доступний там, де є Інтернет; мультимедійність, що передбачає використання майже всіх видів передачі (текст, фото, звук, відео, графіка). Крім того, багато традиційних ЗМІ, які перенесли свої версії в електронний формат, мають таку блогову функцію, як коментарі, що дозволяє комунікатору відстежити ефект свого повідомлення у цільової аудиторії.

Головною перевагою соціальних мереж, на відміну від електронних ЗМІ, є міжнародний фактор – загальнодоступність. Якщо електронне видання має свою цільову аудиторію, соціальні мережі об'єднують усіх за рахунок міжнародного статусу. Саме тому вони почали впливати не лише на міжнародну цільову аудиторію, а й на самих стратегічних комунікаторів.

Соціальні мережі, такі як Facebook, Twitter, стали улюбленим інструментом у політичних лідерів у їхніх публічних дискусіях з міжнародною аудиторією. Так, Twitter створив найпопулярніший на даний момент Інтернет-майданчик, де користувачі можуть висловлювати свої невдоволення та бути почутими. У цьому сенсі показовими є протести проти результатів виборів в Ірані в червні 2009 року, на яких було проголошено перемогу Махмуда Ахмадінежада. Тисячі іранців вийшли тоді на вулиці, вигукуючи на адресу Ахмадінежада закиди щодо фальсифікації підсумків голосування. Головним електронним каналом їх обурення став Twitter. Під хеш-тегами #IranElection іранські користувачі Twitter з секундним проміжком викладали новини про демонстрації на вулицях Тегерана та інших міст. Голос народу, що вмістився в 140 знаків, на якийсь час проклав собі шлях у вільну пресу через Інтернет-цензуру Ірану. Twitter став символом іранського повстання, і сервіс коротких новин був номінований на Нобелівську премію миру [10].

Також треба зазначити, що Twitter та Facebook відіграли головну роль у запобіганні соціальному конфлікту у Венесуелі наприкінці 2012 – на початку 2013 року. Акції протесту, що прокотилися країною через довгу відсутність інформації про стан здоров'я чинного президента країни Уго Чавеса, були значною мірою припинені після виходу останнього на зв'язок з цільовою аудиторією країни через Twitter [11].

Варто розуміти, що хоч суть поняття «стратегічні комунікації» є загальною для всіх акторів міжнародних відносин, кожна країна і організація додає нові ознаки у визначення і розуміє його по-своєму. Одним із найяскравіших представників міжнародних відносин, що активно використовує систему стратегічних комунікацій для зв'язку з громадськістю і досягнення своїх цілей, є НАТО. Сама організація визначає стратегічні комунікації як скоординоване та належне використання комунікаційних заходів і можливостей НАТО для підтримки політики, операцій і діяльності Альянсу, а також для досягнення цілей НАТО.

Ці види діяльності та можливості передбачають наступне:

– громадську дипломатію, яка включає заходи НАТО з комунікації та інформаційно-роз'яснювальної роботи серед цивільного населення, відповідальні за

підвищення обізнаності та формування розуміння та підтримки політики, операцій і діяльності НАТО, на додаток до національних зусиль членів Альянсу;

– зв'язки з громадськістю: участь цивільних НАТО через засоби масової інформації для своєчасного, точного, оперативного та ініціативного інформування громадськості про політику, операції та діяльність НАТО.

– військові зв'язки з громадськістю: популяризація військових цілей і завдань НАТО серед аудиторії з метою підвищення обізнаності та розуміння військових аспектів Альянсу;

– інформаційні операції: військові консультації НАТО та координація військової інформаційної діяльності з метою створення бажаного впливу на волю, розуміння та можливості супротивників та інших сторін, затверджених договором, для підтримки операцій, місій і цілей Альянсу;

– психологічні операції: запланована психологічна діяльність з використанням методів комунікації та інших засобів, спрямована на затверджену аудиторію з метою впливу на сприйняття, ставлення та поведінку, впливаючи на досягнення політичних і військових цілей.

НАТО розробило систему стратегічних комунікацій з метою:

– робити позитивний і безпосередній внесок у досягнення успішного виконання операцій, місій і заходів НАТО шляхом включення стратегічного комунікаційного планування в усе оперативне та політичне планування;

– розвивати, у тісній і тривалій координації з країнами НАТО, громадську обізнаність, розуміння та підтримку конкретної політики НАТО, операцій та інших заходів серед усіх відповідних аудиторій;

– сприяти загальній обізнаності та розумінню діяльності організації в рамках ширших і постійних зусиль громадської дипломатії [12].

Отже, стратегічна комунікація – це процес передачі єдиного повідомлення через публічні дипломатичні канали, зв'язки з громадськістю (представники уряду) та інформаційні/психологічні операції. Сьогодні все більше міжнародних акторів (країн, а також і міжнародних організацій) практикують застосування стратегічних

комунікацій задля досягнення своїх цілей на світовій арені і отриманні підтримки їх політики. Основними каналами передачі повідомлень стратегічних комунікацій в еру глобалізації стають сучасні технології, зокрема мережа Інтернет і популярні соціальні платформи.

## 1.2.Історія становлення та трансформація інституту стратегічних комунікацій Північноатлантичного Альянсу

НАТО було створено в 1949 році як військово-політичний блок, який був заснований на базі Західної Європейської Угоди (ЗЄУ) з метою захисту європейських країн від радянської агресії. Стаття 5 Вашингтонського договору визначає «колективну оборону» як основне завдання Альянсу [13].

Під час Холодної війни політика НАТО щодо оборони та стримування зосереджувалася переважно на жорсткій силі. У цей час інформаційна політика відігравала додаткову і здебільшого непомітну роль, оскільки стримування базувалося головним чином на розробці та розгортанні систем озброєнь і військових підрозділів на території НАТО, особливо в Європі. Інформаційна політика була сформована в основному традиційними засобами масової інформації, керованими державами, і обидві сторони, НАТО та Варшавський договір, прагнули інформувати власне населення, а не впливати на іншу сторону.

Проте зародження системи стратегічних комунікацій в НАТО розпочалось ще 18 травня 1950 року, коли Північноатлантична рада, найвищий керівний орган НАТО, випустила резолюцію, в якій зобов'язалася: «заохочувати та координувати публічну інформацію для досягнення цілей Договору, залишаючи відповідальність за національні програми кожному з країн» [14]. Це певною мірою вдалося зробити.

А от сама історія становлення інституту стратегічних комунікацій Північноатлантичного Альянсу (НАТО) починається з 1951 року, коли було створено Комітет інформації НАТО з метою забезпечення координації інформаційних дій між країнами-членами. Протягом наступних років Комітет

інформації НАТО працював над розробкою загальної стратегії комунікацій та забезпеченням консистентної інформаційної політики в рамках Альянсу.

У 1990-х роках, коли завершилась Холодна війна, НАТО стикнулося з новими викликами та загрозами. Суспільство стало більш розпаленим і більш вимогливим до здійснення зовнішньої політики національними урядами. Військова та політична відповідь на ці виклики була недостатньою. У цьому контексті постала потреба в удосконаленні комунікації та стратегій для впевненості в тому, що національні громадяни розуміють, чому НАТО потрібне і як воно забезпечує їхню безпеку [15].

Тобто, з одного боку, відбувся швидкий розвиток комунікаційних технологій, а з іншого – важливі зміни в завданнях Альянсу. НАТО розпочала нові місії, такі як операції з розбудови нації в Боснії чи Косово, які стосувалися прав людини або невійськових питань. Таким чином, НАТО відчула необхідність зосередитися на комунікації, особливо з використанням сучасних технологій, щоб вчасно та правильно інформувати громадськість і забезпечити усі місії. Департаменти зв'язків з громадськістю та публічної політики в НАТО були сформовані відповідно до цих нових вимог. Роль публічної дипломатії як щодо «старих держав-членів», так і щодо нових держав, які прагнуть вступити в НАТО, а також щодо десятків нових партнерів НАТО по всьому світу призвела до активніших зусиль щодо охоплення цієї аудиторії.

Атаки 11 вересня 2001 року стали важливим поворотним пунктом у вже мінливому стані проблем міжнародної безпеки та міжнародної політики загалом. Цей інцидент не тільки вивів «Аль-Каїду» на перший план міжнародного порядку денного, але й зробив Афганістан центральним театром боротьби з тероризмом. Ці події вкотре наголосили на необхідності ефективної комунікації та зв'язків з громадськістю в умовах загострення безпекових загроз. Цей процес також збігся зі спробами НАТО пристосуватися до нових обставин і викликів епохи після Холодної війни. Альянс активізував свою діяльність у ЗМІ, а також зміцив команди зі зв'язків з громадськістю/громадської дипломатії.

У 2003 році було створено Відділ громадської дипломатії НАТО шляхом об'єднання Інформаційного офісу НАТО з його прес-службою. У рамках нової

структури Північноатлантична рада та Генеральний секретар НАТО забезпечували загальне керівництво комунікацією та публічною дипломатією НАТО, що випливає з політичних рішень. НАТО працює в комітетах, що складаються з держав-членів, оскільки всі рішення приймаються консенсусом. Комітет громадської дипломатії НАТО діє як дорадчий орган Ради у сферах комунікації, залучення громадськості та засобів масової інформації. Сильні кампанії публічної дипломатії, які проводяться окремими країнами та за підтримки Відділу громадської дипломатії НАТО, принесли новий досвід і розширили його роль в управлінні своїми програмами публічної дипломатії.

Через складність інформаційної діяльності НАТО почала розробляти свою концепцію StratCom у 2009 році, коли вона визначила StratCom як «скоординоване та належне використання комунікаційної діяльності та можливостей НАТО для підтримки політики, операцій та діяльності Альянсу з метою досягнення цілей НАТО». Концепція розроблена для забезпечення того, щоб аудиторія отримувала чітку, точну та відповідну інформацію щодо дій, а також щоб інтерпретація повідомлень Альянсу не залишалася виключно на волю супротивників НАТО чи інших аудиторій. Згідно з Військовою концепцією 2010 року (2010), StratCom НАТО має на меті забезпечити, щоб аудиторія отримувала «правдиве, точне та своєчасне повідомлення, яке дозволить їм зрозуміти та оцінити дії та наміри Альянсу».

У 2014 році було створено нову структуру – Центр стратегічних комунікацій НАТО (Strategic Communications Centre of Excellence), який базується в Ризі, Латвії. Цей центр є головною точкою для розробки та впровадження стратегій комунікацій в рамках НАТО, включаючи курси підготовки, навчання та дослідження в галузі стратегічних комунікацій [16].

Інститут стратегічних комунікацій (ІСК) Північноатлантичного Альянсу (НАТО) відповідає за розробку та координацію стратегій комунікацій для підтримки місій та операцій НАТО. Основні функції та завдання ІСК ПА включають:

– розробку стратегій комунікацій: ІСК ПА розробляє стратегії комунікацій для підтримки місій та операцій НАТО. Ці стратегії визначають способи, якими НАТО може взаємодіяти з громадськістю, ЗМІ та іншими зацікавленими сторонами;

– координацію зусиль: ІСК ПА координує зусилля інших відділів та організацій НАТО, щоб забезпечити взаємодію між ними та виконання загальної стратегії комунікацій;

– моніторинг і аналіз: ІСК ПА здійснює моніторинг та аналіз інформації, яка відноситься до НАТО, щоб визначити позиції та перспективи громадської думки та відповідність повідомлень НАТО;

– розвиток комунікаційної інфраструктури: ІСК ПА сприяє розвитку комунікаційної інфраструктури НАТО, зокрема, розробляє та підтримує сайти, соціальні мережі та інші засоби комунікації;

– тренінги та освіту: ІСК ПА проводить тренінги та надає освіту з комунікацій для представників НАТО та партнерів;

– розробку повідомлень та матеріалів: ІСК ПА розробляє та публікує повідомлення, прес-релізи, заяви, інтерв'ю, статті, брошури, відео та інші засоби масової комунікації [17].

За багато років свого існування Інститут стратегічних комунікацій Північноатлантичного Альянсу постійно розвивався та адаптувався до нових викликів і вимог.

У 2015 році ІСК ПА розширив свою діяльність і став надавати послуги зі стратегічних комунікацій для усіх країн-членів НАТО. Також у 2015 році було відкрито офіс ІСК ПА в Німеччині, що дозволило Інституту розширити свої можливості у розробці та впровадженні комунікаційних стратегій.

У 2016 році ІСК ПА було офіційно визнано як ключовий організатор інформаційної діяльності НАТО. Також у цьому році було прийнято рішення про розширення мандату Інституту на розробку стратегій у сфері протидії дезінформації.

У 2018 році ІСК ПА почав розвивати співпрацю з іншими організаціями та установами, що займаються стратегічними комунікаціями. Зокрема, Інститут підписав угоди про співпрацю з Європейською службою зовнішньої дії та Державним департаментом США.

У 2019 році ІСК ПА відкрив офіс у Польщі, що дозволило Інституту збільшити свою присутність у Центральній та Східній Європі, та поширити свої дослідження на цей регіон. Зокрема, це сприятиме розвитку взаємодії з країнами Вишеградської групи, які стали важливими членами НАТО та активно беруть участь в різних місіях та операціях Альянсу [18].

Інститут стратегічних комунікацій Північноатлантичного Альянсу виконує ключову роль у сучасному світі, допомагаючи Альянсу зберігати безпеку та стабільність у міжнародному співтоваристві. ІСК ПА виконує низку функцій та завдань, що сприяють досягненню цієї мети.

Однією з головних ролей ІСК ПА є сприяння зміцненню зв'язків між Північноатлантичним Альянсом та громадськістю. Інститут розробляє та реалізує стратегії комунікації, спрямовані на забезпечення відкритості, прозорості та взаємодії з громадськістю. Це включає в себе забезпечення широкого доступу до інформації про діяльність Альянсу та його політики, а також налагодження діалогу з представниками громадськості, в тому числі через організацію конференцій та заходів.

Іншою важливою роллю ІСК ПА є підтримка інформаційної безпеки. Інститут веде моніторинг та аналіз інформації в міжнародному просторі, а також розробляє та впроваджує стратегії комунікації з метою захисту від дезінформації та забезпечення правдивої інформації. Також ІСК ПА сприяє розвитку засобів та технологій для боротьби зі штучно створеною дезінформацією та кіберзагрозами.

Окрім цього, Інститут є ключовим інструментом у веденні дипломатичної діяльності Альянсу. Це пов'язано з тим, що ІСК ПА займається розвитком та реалізацією стратегій комунікації Альянсу з громадськістю, медіа та партнерами. Він також координує зусилля Альянсу щодо відповіді на дезінформацію та інші загрози безпеці, пов'язані з інформаційною війною.

Інститут стратегічних комунікацій ПА активно співпрацює з громадськістю та іншими зацікавленими сторонами, щоб забезпечити належне розуміння місії та завдань Альянсу, а також допомагає зміцнювати довіру до нього. Крім того, він займається підготовкою та проведенням кампаній з просвітницької діяльності,

наукових конференцій, семінарів та інших заходів для підвищення рівня свідомості про цінності та місію Альянсу серед широкого загалу.

Інститут стратегічних комунікацій ПА є важливим інструментом у боротьбі з дезінформацією та іншими загрозами безпеці, пов'язаними з інформаційною війною. Зокрема, ІСК ПА координує роботу Альянсу щодо виявлення та аналізу дезінформації, а також розробляє та впроваджує заходи для попередження та протидії таким загрозам. Він також активно співпрацює з міжнародними партнерами у цій сфері.

На тлі війни Росії в Україні та загострення риторики проти Заходу з боку Кремля НАТО і його підрозділи, серед яких Інститут стратегічних комунікацій, завершує реформу спільної стратегії протидії як російській загрозі, так і терористичним групам. Його структура, створена для відповіді на нові геополітичні реалії та прискорена вторгненням Москви, є найбільшою реконфігурацією з часів Холодної війни. Документ, який займає близько 4000 сторінок, описує першу повну та єдину реформу доктрини НАТО за три десятиліття. Серед пропозицій – зміни у військовій стратегії Альянсу – відхід від широкомасштабних втручань і надання пріоритету розгортанню невеликих батальйонів і регіональних експертів – і його методи аналізу та надання оновленої інформації про різноманітні загрози з боку Кремля, серед яких військові, кібератаки та гібридні атаки, а також відповідь НАТО на ці сценарії [19].

Останній саміт НАТО, який відбувся в червні 2022 року в Мадриді, оголосив Російську Федерацію «найзначнішою та прямою загрозою безпеці членів Альянсу, а також миру та стабільності в євроатлантичному регіоні» та закликав до значного зміцнення оборони, прискорення розвитку регіональних планів. На Мадридському саміті, який відбувся 28-30 червня 2022 року, члени НАТО прийняли нову Стратегічну концепцію, яка має на меті визначити бачення Альянсу на наступне десятиліття. Стратегічну концепцію НАТО до 2022 року було розроблено в особливий історичний момент, ознаменований вторгненням Росії в Україну в лютому 2022 року. Зважаючи на це, нова Концепція свідчить про чітку еволюцію у визначенні Альянсом пріоритетів його основних завдань: оборони та стримування та

покінчення з ілюзією партнерства з Росією. У розділі під назвою «Стратегічна концепція НАТО в тіні війни» він обговорює зміну підходу НАТО до Росії після її агресії проти України, нове визначення Китаю, наголос на гібридній війні, зміні клімату та підтримці Альянсу технологічний край [20].

Отже, StratCom НАТО є не просто черговою технологічною розробкою, а відображенням та відповіддю в епоху інформації і її виклики. Створення Інституту стратегічних комунікацій стало відправною точкою для створення позитивного іміджу організації, сумісного з її внутрішньою структурою, місією та баченням. З огляду на щоденні події та зміни концепцій політичної безпеки в усьому світі, важливо, щоб НАТО була представлена громадськістю та сприймалася як організація високої доброчесності, яка має єдину та скоординовану політику та робочі завдання.

### 1.3.Інституційний та нормативно-правовий вимір реалізації інформаційно-комунікативної політики організації

Стратегічна комунікаційна діяльність НАТО була активізована терористичними атаками 11 вересня 2001 року та військовою кампанією в Афганістані, що продемонструвало важливість зусиль з пояснення своїх дій та операцій у регіонах, включно з місцевим населенням. У 2007 році у Верховному штабі об’єднаних сил НАТО в Європі було створено Управління стратегічних комунікацій, щоб переконати європейську громадськість у правильності дій європейських країн Альянсу в Афганістані. У наступні роки з’явилися доповіді та заяви зі стратегічних комунікацій (зокрема, «Політика стратегічних комунікацій НАТО», «Удосконалення стратегічних комунікацій НАТО»).

У Декларації саміту НАТО в Страсбурзі (2009) чітко зазначено, що «для Альянсу стає все більш важливим повідомляти про зміну своєї ролі, цілей і місій належним, своєчасним, точним і активним чином. Стратегічні комунікації є невід’ємною частиною наших зусиль для досягнення політичних і військових цілей

Альянсу». Відтоді розпочався процес розвитку стратегічних комунікацій у діяльності Північноатлантичного альянсу в нормативному та інституційному вимірах [21].

У 2014 році в Ризі розпочинає роботу Центр передового досвіду стратегічних комунікацій НАТО (або «NATO StratCom COE»). До його завдань входить: розробка програм сприяння розвитку та гармонізації доктрини стратегічних комунікацій; проведення досліджень та експериментів для пошуку практичних рішень існуючих проблем; «винесення уроків» із застосування стратегічних комунікацій під час військової операції іони; збільшення навчальних і освітніх зусиль і можливостей взаємодії [22].

Функціонування стратегічних комунікацій в НАТО передбачає визначення чіткої інституційної структури та відповідальності для кожного компонента цієї структури. Відповідно, можна говорити про систему стратегічних комунікацій Альянсу.

Перш за все, слід зазначити, що діяльність у сфері стратегічних комунікацій має значні структурні наслідки, оскільки спрямована на сприяння взаємодії між різними інституціями, які здійснюють інформаційно-комунікаційну діяльність. Водночас такі зміни нелегкі, особливо в умовах тривалого функціонування вертикальної ієрархічної структури управління.

Одним із лідерів є Північноатлантична рада, яка забезпечує загальне керівництво стратегічними комунікаційними зусиллями НАТО та надає конкретні стратегічні та політичні вказівки щодо інформаційних і комунікаційних можливостей Альянсу. Керівництво включає Генерального секретаря, який фактично є головним представником НАТО і викладає конкретні стратегічні послання для всіх цивільних і військових органів НАТО щодо політики Альянсу. Більш конкретні функції покладаються на помічника Генерального секретаря з публічної дипломатії, який повністю відповідає за стратегічні комунікації від імені Генерального секретаря. Він наглядає, серед іншого, за координацією всіх стратегічних комунікаційних заходів у всіх цивільних і військових органах і командуванні НАТО, а також спрямовує всі заходи публічної дипломатії для

забезпечення координації та синхронізації. У свою чергу речник Альянсу від імені Генерального секретаря забезпечує повсякденне управління всією інформаційною діяльністю в штаб-квартирі НАТО та забезпечує відповідність усіх повідомлень і комунікаційної політики НАТО політичним настановам і рішенням.

Існує також три рівні відповідальності за формування стратегічної комунікаційної політики Альянсу, які формулюються таким чином:

1. Повідомлення, що передають цілі НАТО, визначаються на рівні штаб-квартири НАТО, зокрема вищезгаданої Північноатлантичної ради, Генерального секретаря та Військового комітету (останній стежить за відповідністю політичних дій і рішень військовій політиці НАТО та забезпечує суто військовою консультацією Північноатлантичну раду).

2. Тоді стратегічні комунікації визначаються на рівні Верховного штабу об'єднаних сил НАТО в Європі (SHAPE), але під керівництвом штабу Альянсу. На цьому рівні, відповідно, конкретизується концепція стратегічних комунікацій, включаючи їх цілі та необхідні ресурси для їх реалізації. Також на цьому рівні є відповідальність за впровадження навчальних програм зі стратегічних комунікацій.

3. Нарешті, третій рівень – це рівень командирів підрозділів, які гарантують, що всі комунікації (усні, письмові, навіть поведінкові) передають повідомлення, розроблені в штаб-квартирі НАТО (перший рівень). На відміну від попередніх двох рівнів, які мають фактично стратегічний характер, цей є оперативно-тактичним [23].

Якщо завдання нижнього рівня структури стратегічних комунікацій більш-менш зрозумілі, то специфіка стратегічної діяльності в комунікаційному контексті потребує уточнення. Документи НАТО визначають завдання Керівництва зі стратегічних комунікацій таким чином:

1. Аналіз інформаційного середовища. Його передумовою є ситуаційна обізнаність, яка визначає можливості та ризики та створює основу для оцінки ефективності стратегічних комунікацій. Аналіз інформаційного середовища є міждисциплінарним безперервним завданням, яке виконують навчені співробітники. При цьому результати цієї аналітичної роботи мають бути сформульовані доступно, щоб бути корисними.

2. Формування бажаних наслідків. Йдеться про моделювання обставин і методів, за яких зусилля НАТО зі стратегічної комунікації принесуть результати, необхідні для Альянсу. Зазначається, що ця діяльність вимагає глибоких знань інформаційного середовища, цілей і завдань конкретної місії НАТО, а також наявних ресурсів для оцінки відповідних наслідків тих чи інших дій. Таким чином, це завдання безпосередньо пов'язане з попереднім – аналізом інформаційного середовища.

3. Сприяння цілепокладання. Справа в тому, що всі дії так чи інакше впливають на інформаційний простір: позитивно (якщо скорочується розрив між словами і діями) або негативно (якщо, наприклад, повідомлення для внутрішньої та зовнішньої аудиторії відрізняється за змістом). Тому необхідно звести до мінімуму негативні наслідки і максимізувати позитивні.

4. Планування діяльності. Це завдання стосується залучення у разі потреби підрозділів планування інформаційних операцій.

5. Інтеграція комунікаційної діяльності. Ефективна комунікація потребує гармонізації та синхронізації комунікаційних зусиль на різних рівнях; крім того, діяльність, спрямована на створення певних наслідків в інформаційному просторі, також повинна враховувати контекст усіх інших дій у рамках конкретної місії чи операції.

6. Комунікаційна залученість. Пряме спілкування допомагає встановити прозорість, довіру та автентичність. Тому такі дії третього, тактико-оперативного рівня структури стратегічних комунікацій мають бути ретельно сплановані. А оскільки керівники комунікацій НАТО одночасно є комунікаторами (наприклад, Генеральний секретар і речник Альянсу), необхідно детально планувати їхні дії, щоб синхронно доносити правильні повідомлення до союзників.

7. Спілкування в ЗМІ. НАТО має власні медіа-ресурси і може використовувати сторонні медіа різними способами, від розміщення в них реклами до впровадження вбудованої журналістської програми. Складність полягає в тому, що інформація, яка потрапила в медіапростір з боку Альянсу, вже не підконтрольна йому, а тому такий

формат комунікації потребує належної організації для дотримання вимог прозорості, підзвітності та достовірності.

8. Оцінка впливу. Йдеться про визначення ефективності комунікації, її відповідності цілям і завданням операції чи місії НАТО, а також формулювання висновків щодо її подальшого вдосконалення.

9. Освіта та навчання. Ця функція переходить зі стратегічного на оперативний і тактичний рівні в рамках стратегічної комунікаційної системи НАТО. Необхідно не лише нарощувати необхідні людські ресурси для безпосереднього виконання конкретних операцій чи місій НАТО, а й підтримувати спадкоємність у групі спеціалістів, які займаються стратегічними комунікаціями Альянсу [24].

Як уже зазначалося, поштовхом для формування комунікаційної політики НАТО у стратегічному вимірі стали події 2001 року, які показали слабкість діяльності Альянсу в цьому вимірі. Саме тому перші пілотні моделі стратегічних комунікацій почали формуватися в рамках Міжнародних сил сприяння безпеці (МССБ), об'єднаних сил сприяння безпеці в Афганістані, головним завданням яких було створення мирної та стабільної обстановки для надання допомоги країні в поствоєнній відбудові, а також недопущення відновлення там терористичної діяльності.

В рамках МССБ першою проблемою у функціонуванні стратегічних комунікацій НАТО була організаційна проблема. Вище зазначалося, що вони включають публічну дипломатію, публічну політику, військову публічну політику, інформаційні операції та психологічні операції. Питання полягало в тому, як забезпечити координацію таких різноманітних напрямків діяльності, в тому числі на оперативно-тактичному рівні.

Так, на початку доктрини НАТО було визначено, що державною військовою політикою керує безпосередньо керівник підрозділу, який бере участь у конкретній місії чи операції, тоді як інформаційно-психологічні операції покладаються на окрему структуру – Оперативне бюро (J3), яка координує свою діяльність з командуванням через координатора стратегічних комунікацій [25].

З одного боку, ця структура розрізняла психологічні операції та військову громадськість політики, яка відповідала основним документам НАТО, з іншого боку, ускладнювала координацію діяльності стратегічних комунікацій, як це передбачено їх визначенням. Тому згодом його було реорганізовано: усі три компоненти стратегічних комунікацій (інформаційні операції, психологічні операції та військова громадська політика) перейшли фактично під опіку Оперативного бюро (замість J3 стало називатися Joint Effects), але безпосередня координація військових Державною політикою займався вже командир частини. Це як для виконання вимог доктрини НАТО, так і для підвищення ефективності координації.

Далі почали формуватися більш компромісні механізми організації стратегічних комунікацій в рамках МССБ. Справа полягала в тому, що більшість держав Альянсу не бажали узгоджувати інформаційно-психологічні операції з військовою державною політикою. Справа в тому, що якщо перші два компоненти StratCom безпосередньо супроводжують бойові дії, то третій використовується в мирних цілях. Тому запропоновано структуру, в якій координація військової публічної політики здійснюється через окремого речника, який отримує вказівки як від командувача, так і від заступника начальника штабу зі зв'язку (замість Joint Effects). Останній також відповідає за інформаційно-психологічні операції.

Поштовхом до спрямування стратегічних комунікаційних зусиль та їх масштабування стало посилення деструктивного інформаційного впливу Російської Федерації у 2014 році, що вилилось у нетрадиційну, гібридну війну проти України зокрема та Європейського континенту та НАТО загалом. На рівні керівництва НАТО визнала ці загрози та почала формувати спільне бачення StratCom, зокрема в інституційній та функціональній сферах [24].

Отже, сьогодні можна констатувати відсутність суттєвих протиріч у реалізації стратегічної комунікаційної політики в Північноатлантичному альянсі. Відповідно до доктринальних документів та існуючих інститутів НАТО сформовано трирівневу структуру управління StratCom, яка забезпечує як загальне управління цією сферою на стратегічному рівні, так і її реалізацію на тактичному та оперативному рівнях. Водночас процес формування єдиного наративу, який Альянс бачить як ключ до

успіху стратегічних комунікацій, все ще триває через його вартість і потребу в додатковому часі. У довгостроковій перспективі це може допомогти сформувати новий імідж НАТО як глобальної інституції безпеки, відповідної сучасному світу та найважливішим для неї загрозам безпеці.

Можна зробити висновки, що стратегічна комунікація – один із інструментів зовнішньополітичної комунікації, який полягає у використанні спланованих та скоординованих повідомлень, ідей, каналів комунікації для цілеспрямованого впливу на цільову аудиторію з метою досягнення національних цілей та просування національних інтересів, також інтересів різних акторів міжнародних відносин, в тому числі і міжнародних організацій.

Стратегічні комунікації НАТО – це скоординоване та належне використання комунікаційних заходів і можливостей НАТО для підтримки політики, операцій і діяльності Альянсу, а також для досягнення цілей НАТО. Цей підрозділ організації почав формуватись як відповідь на світові виклики безпеці і розвиток інформаційних технологій. Загальна мета комунікаційної діяльності НАТО полягає в тому, щоб сприяти діалогу та взаєморозумінню, одночасно сприяючи обізнаності громадськості з питань безпеки та сприяючи залученню громадськості до безперервного процесу обговорення питань безпеки.

# РОЗДІЛ 2
# ОСНОВНІ МЕХАНІЗМИ ТА ЗАСОБИ ДІЯЛЬНОСТІ НАТО В ГАЛУЗІ ІНФОРМАЦІЇ

## 2.1. Механізми та засоби практичного здійснення стратегічних комунікацій Північноатлантичного Альянсу

Стратегічні комунікації є відносно новим явищем у теорії та практиці міжнародної політики, що стосується сфери зовнішньої політики держав і міжнародних організацій. Концептуальною основою стратегічних комунікацій є скоординований вплив на конкретні цільові аудиторії за допомогою комплексу дій, підкріплених інформаційною діяльністю відповідних акторів. Сучасний спосіб життя, який розглядається з точки зору доступності та передачі інформації, вимагає цілодобової роботи осіб в організації, які відповідають за цей процес. Що стосується НАТО, то створення мережі зв'язку значною мірою впливає на дії НАТО, особливо з точки зору того, як це буде сприйнято громадськістю. Громадське сприйняття є особливо важливим і впливає на успіх операцій і політики НАТО. НАТО має використовувати різні канали, а саме традиційні медіа та Інтернет-ЗМІ; воно повинне залучати громадськість до управління та діяльності з метою підвищення обізнаності, щоб вони могли зрозуміти та підтримати його рішення та операції. Це вимагає інституційного підходу та високого рівня координації між державами-членами та країнами-партнерами, тобто між відповідними акторами, відповідно до процедур, політики та принципів НАТО.

Ефективна стратегічна комунікаційна політика в рамках альянсу НАТО вимагає:

- чітких цілей стратегічних дій НАТО у сфері комунікацій;
- відповідності основним принципам стратегічної комунікації НАТО;
- зв'язку між різними інформаційними напрямками в НАТО (публічна дипломатія, цивільні зв'язки з громадськістю, військові зв'язки з громадськістю, інформаційні операції та психологічні операції) [17].

– чіткого визначення ролі та повноважень залучених учасників, відповідальних за комунікаційний процес в НАТО.

Насправді стратегічні комунікації являють собою значну частину внутрішнього зобов'язання щодо досягнення політичної безпеки та підтримки ефективного військового альянсу.

Основні принципи та ключові стратегічні комунікації НАТО стосуються:

– однакового оцінювання повідомлення в усіх сферах, де воно передається;

– моніторингу швидкості передачі інформації та забезпечення її актуальності та корисності;

– чіткості і точності повідомлення;

– ефективності з точки зору ефекту переданої інформації – тобто досягнення бажаної мети;

– аналізу громадської думки та процесу адаптації політики Альянсу щодо ставлення громадськості до представлених питань [27].

Північноатлантична рада надає повну підтримку процесу стратегічних комунікацій в НАТО. Однак для того, щоб успішно досягти цього процесу, необхідно регулярно досягати стратегічного потоку інформаційних дій. Відповідно до цілей і принципів, описаних вище, існує роль генерального секретаря, а також головного речника Альянсу. Однак Північноатлантична рада дає точні вказівки щодо політичних напрямів і рішень не лише генеральному секретареві, а й Військовому комітету.

Особливо важливо підтримувати контрольовану функцію радника зі зв'язків із громадськістю, оскільки особа, яка відповідає за цю сферу, забезпечує координацію та взаємодію між стратегічними командуваннями та стратегічними операціями.

Проте, коли йдеться про взяття на себе конкретних обов'язків щодо комунікаційного процесу, який здійснюється в НАТО, максимальна ефективність дій Північноатлантичної ради та Генерального секретаря є обов'язковою. Крім того, державам-членам необхідно поважати обов'язки одна одної та забезпечити постійну координацію з метою побудови спільноти шляхом передачі інформації. Це

сприятиме легшій реалізації операцій, плануванню та партнерству між державами та їхніми представниками.

Необхідно надати додаткові вказівки всім органам і особам, залученим до процесу створення довгострокової та успішної комунікаційної стратегії для НАТО, особливо у сфері соціальних медіа. Але коли мова йде про ЗМІ з величезним авторитетом і впливом, організація повинна працювати відповідно до медіа-програми, водночас відповідаючи власним можливостям. Для цього необхідно бути в курсі всіх нововведень соціальних мереж, за допомогою яких вони можуть використовуватися для обговорення поточних подій і подій, в яких бере участь організація, а також для реклами повсякденної діяльності. Проте правління НАТО має бути обережним, користуючись соціальними мережами, щоб не поставити під загрозу оперативну та організаційну безпеку. Вони повинні бути обережними, щоб не передавати новини та конфіденційну інформацію через соціальні мережі, особливо якщо вони пов’язані з питаннями безпеки.

Привернення уваги до процесу стратегічної комунікації в НАТО є особливо важливим через спосіб контролю вихідних повідомлень. Він призначений не лише для внутрішнього населення держав-членів, а й для іноземного населення, яке включає як союзників, так і ворогів. Йдеться про створення відповіді на виклики навколишнього середовища, яке базується на безлічі інформації, до якої може миттєво отримати доступ кожен.

Контроль інформації також важливий у міжурядовій комунікації НАТО та за її межами. Крім того, у цьому контексті необхідно звернути увагу на концепцію міжвідомчого потоку інформації всередині самого уряду. Точніше, стратегічну комунікацію необхідно розглядати на глобальній основі та сегментувати в межах інституцій держав-членів, країн-партнерів і в самій організації. Насправді, головна мета стратегічних комунікацій НАТО полягає в тому, щоб сприяти поведінці цільової аудиторії, яка подобається акторам, залученим до комунікації.

Стратегічні комунікації НАТО мають на меті покращити імідж організації та заохотити поведінку аудиторії, спрямовану на підтримку Альянсу. Тобто

спілкування в цьому контексті не сприяє лише впливу на сприйняття громадськості, але й впливу на поведінку громадськості.

Щоб досягти ефективної передачі інформації в потрібний час і в потрібному місці, а також концептуалізувати та досягти основних цілей організації, необхідно переглянути процес передачі інформації. Це означає, що внутрішня ієрархія НАТО іноді ускладнює процес отримання якісної та своєчасної інформації. З цією метою необхідно, щоб більше осіб з організації було залучено до процесу комунікації, щоб зробити процес більш плавним на основі попередньо встановлених правил і процедур.

А також необхідно розуміти, якими інструментами і тактиками користується Стратком НАТО для здійснення процесу стратегічних комунікацій. Найперший і найпоширеніший канал для передачі інформації – електронна пошта або телефон. Коли існують особисті стосунки, такому спілкуванню надається перевага. Ці засоби можна також використовувати для спілкування з ключовою аудиторією, де немає особистих стосунків, але участь необхідна для успіху проекту. Ключова аудиторія для використання усих інструментів – внутрішні-зовнішні, професійні та непрофесійні стейкхолдери.

Наступна опція – особисті візити. Вона доступна також, коли існують особисті стосунки. Особисті візити також можуть здійснюватися з метою маркетингу проекту до незалучених зацікавлених сторін за межами типових каналів зв’язку, таких як урядові організації, неурядові організації, міжнародні організації, університети тощо.

Ще один варіант здійснення стратегічних комунікацій в НАТО – конференції і семінари. Залежно від мети семінару/практикуму запрошуються різні цільові аудиторії. Звісно, перевага віддається поєднанню учасників із усіх цільових аудиторій для заохочення спілкування.

Веб-сайт – ще одна можливість, яку використовує НАТО для розповсюдження інформації серед цільової аудиторії. Тут Альянс має декілька варіантів: Інтранет, який містить корисну інформацію для членів організації; Екстранет відкриває можливості для розміщення, обміну та розповсюдження інформацією серед членів

Організації через портал, захищений паролем. І Інтернет – місце, де інформація буде розміщена для всіх охочих її прочитати. Результат ефективності використання такого способу буде вимірюватись підрахунком кількості і активності користувачів, відгуками користувачів, статистикою відвідувань, рейтингом пошукової системи.

Брошури також є в арсеналі Альянсу як метод здійснення комунікації з аудиторією. Їх можна роздавати/встановлювати на конференціях, семінарах, засіданнях робочих груп та під час особистих візитів членам усіх цільових аудиторій. З тієї ж групи – інформаційні бюлетені, які можуть надсилатися поштою відповідним цільовим аудиторіям на регулярній основі. Вони повинні містити календар з важливими подіями, які відбудуться протягом наступних 2-4 місяців

Прес-релізи, що розміщуються в газетах і журналах, в яких міститься інформація про проведені заходи. Ці прес-релізи повинні або розповідати історію, пов'язану з аудиторією ЗМІ, або надавати інформацію про проведену/майбутню подію, актуальну для людей у регіоні.

Також Альянс використовує метод висвітлення на телебаченні або радіо, а також в пресі – друкування статей в різних джерелах. Історії успіху та найкращі практичні приклади можуть бути цікавими для ширшої аудиторії, тому їх можна буде опублікувати в інформаційних бюлетенях, журналах або на веб-сайтах, що містять новини. Приклади передового досвіду та цікаві результати проектів, які мають певний науковий рівень, можуть бути опубліковані у вигляді статей у професійній пресі або на професійних сайтах. З цією ж метою Альянс також активно використовує соціальні мережі. Інформація щодо проектів і заходів публікується щотижня. Ці дописи розповідають або надають інформацію про проведену/майбутню подію, актуальну для людей у НАТО чи ключової аудиторії.

Ще один інструмент, що доступний для НАТО – комунікаційні тренінги і тренінги персоналу. Підвищення ефективності спілкування та навичок персоналу для побудови хороших стосунків з колегами та партнерами, формування команди [28].

Отже, Стратком НАТО має в наявності багато різних варіантів для здійснення діяльності. Широке коло інструментів Страткому дозволяє Альянсу залучати

різноманітні канали передачі інформації і охоплювати своїми повідомленнями ширшу аудиторію.

## 2.2. Аналіз стратегічних комунікацій НАТО як дієвого механізму протидії дезінформації

НАТО розглядає дезінформацію як навмисне створення та поширення неправдивої та/або маніпульованої інформації з наміром ввести в оману [29]. Дезінформація має на меті поглибити розбіжності всередині країн Альянсу та між ними, а також підірвати довіру людей до обраних урядів. Альянс має справу з цими проблемами з моменту свого заснування та активно протидіє значному зростанню дезінформації та пропаганди після того, як Росія незаконно анексувала Крим у 2014 році.

НАТО активізувала зусилля з протидії дезінформації, дотримуючись чітких вказівок глав держав і урядів Альянсу в Декларації Брюссельського саміту 2018 року, в якій зазначено: «Ми стикаємося з гібридними викликами, включаючи кампанії з дезінформації та зловмисну кібер-діяльність». У 2019 році у своїй Лондонській декларації глави держав і урядів Альянсу заявили, що НАТО «посилює свою здатність готуватися до гібридної тактики, яка спрямована на підрив нашої безпеки та суспільства, стримувати та захищатися від неї».

Підхід НАТО до протидії дезінформації передбачає подвійну модель, зосереджену на функціях «Зрозуміти» та «Залучити». Функція «Розуміти» включає оцінку інформаційного середовища, яка регулярно відстежує, контролює та аналізує інформацію, пов’язану з місією НАТО. Це дозволяє НАТО оцінити ефективність своїх комунікацій. Функція «Залучити» впроваджує ці знання, дозволяючи НАТО пристосовувати свої стратегічні комунікації до того, щоб найбільш ефективно протидіяти дезінформації [30].

Комунікації НАТО базуються на фактах, є своєчасними, прозорими та скоординованими. Це дозволяє НАТО впливати на суперечливий інформаційний простір. Особливо помітно це проявляється зараз, під час активної фази бойових дій,

які 24 лютого розпочала Російська Федерація в Україні. Окрім розгортання фізичного фронту, держава-агресор веде війну ще й в кіберпросторі. І на цьому полі бою НАТО має дуже важливу і визначальну роль – воно виконує функцію розвінчувача міфів.

Вторгнення Росії в Україну було виправдано системою самовіктимізації, посилаючись на очевидне оточення Росії західними ворогами, які заохочували Україну готувати напади на російських громадян, які проживають на Донбасі, в Криму і навіть на саму Росію. Стверджуючи, що НАТО постачає Україні озброєння саме для цієї мети, російська дезінформація проштовхнула наратив про те, що, підтримуючи Україну, Захід сам готувався напасти на Росію, яка тому вирішила діяти превентивно та атакувати першою, щоб захистити своїх громадян. У цьому наративі українці були значною мірою зневажені, коли президент Росії Володимир Путін пообіцяв «денацифікувати» та «демілітаризувати» «корумповану Україну», захищаючи російські етнічні меншини, які перебувають під загрозою зникнення, і визнаючи їхні претензії на суверенітет [31]. НАТО особливо несе на собі тягар російських спроб дезінформації, коли проросійські традиційні та онлайн-ЗМІ звинувачують його у веденні проксі-війни з Росією в Україні або навіть у спробі завдати ядерного удару під виглядом захисту невинних українців. Хоча основною цільовою аудиторією цих повідомлень, як правило, є російськомовне населення, колишні радянські республіки та навіть інші країни Європи/НАТО були ціллю спроб дезінформації, щоб схилити громадську думку проти України.

Проте гібридна війна Росії проти України розпочалась ще після українського Майдану та анексії Криму в 2014 році і вже тоді Росія намагалася вплинути на громадську думку за допомогою цілеспрямованих кампаній з дезінформації.

Один із наративів, розпочатий ще до війни, був особливо наполегливим: Організація Північноатлантичного договору (НАТО) – європейський і північноамериканський військовий альянс із 30 членами, створений після Другої світової війни – не лише загрожує Росії, але й може навіть планувати вторгнутися в Росію. Задовго до вторгнення в Україну в лютому 2022 року експерти говорили, що Росія поширювала такі історії, щоб виправдати війну. Наприклад, у телевізійному

зверненні за кілька днів до вторгнення президент Росії Володимир Путін заявив, що НАТО «дедалі більше розширюється», хоча інсувала домовленість, що НАТО ніколи не буде розширюватись і брати нових членів. Проте, НАТО одразу відповіло на цей виклик і спростувало цю інформацію. Такої угоди ніколи не укладалося. Двері НАТО були відкриті для нових членів з моменту його заснування в 1949 році – і це ніколи не змінювалося. Ця «Політика відкритих дверей» закріплена в статті 10 засновницького договору НАТО, де сказано, що «будь-яка інша європейська держава, здатна підтримувати принципи цього Договору та сприяти безпеці Північної Атлантики», може подати заявку на членство. Рішення про членство приймаються консенсусом між усіма членами Альянсу [32].

Путін також стверджував, що українці роками вчиняли геноцид проти російськомовних людей у незаконно анексованих «республіках» Донецької та Луганської областей, і що ці території мають бути «денацифіковані».

На початку вторгнення також надходили повідомлення про фінансовані США лабораторії з біозброї в Україні, заяви, які згодом виявилися фальшивими і викриті НАТО. Сюжет про нібито підготовку так званої «брудної бомби» розповсюдило МЗС Росії. «Докази» для заяви були розвінчані; виявилися старі зображення російських АЕС і словенських датчиків диму [33].

Всі ці масштабні кампанії по дезінформації складаються зі щоденних кроків, які Росія робить в сфері ЗМІ і на онлайн-ресурсах. НАТО намагається відслідковувати всі ці дії і за допомогою своїх механізмів і сучасних технологій викривати неправдиві наративи і доносити правду до громадськості. Один із прикладів – нещодавнє відео, що було в мережі в квітні 2023 року. Відео, на якому нібито видно, як люди, названі «українськими нацистами», за допомогою автомобільного відеореєстратора записують інцидент, коли вони зупиняють автомобіль, у якому перевозять жінку з дитиною. Люди нібито стріляли в повітря після того, як жінка не поступилася їм дорогою і розмовляла російською. На іншому відео, опублікованому в Telegram і Facebook, нібито український військовий висловлює невдоволення своїм командуванням. Чоловік у формі стверджує, що зараз разом із однополчанами дислокується в Авдіївці, їх мобілізували з Вінниці на

тиждень. Повідомляється, що вони «три дні були без зв'язку». Крім того, невпізнаний солдат, схоже, заплутаний і невпевнений щодо розташування як ворожих сил («де орки»), так і дружніх військ («де наші»).

НАТО спростувало ці наративи і довело, що перше відео, про яке йде мова, було шахрайським. Його знімали в околицях Донецька, де не могли бути українські сили. Крім того, відео було зняте за допомогою відеореєстратора (заборонений в Україні з березня 2022 року) [34].

Друге відео також було визнане Центром стратегічних комунікацій сфабрикованим. По-перше, всі військовослужбовці строкової служби, які пройшли медичний огляд і визнані придатними до служби, направляються до навчальних центрів на території України. Строк навчання мобілізованих в умовах воєнного стану становить не менше двох місяців. По-друге, солдат на відео не дотримується правил вимови української мови, а натомість має чіткий російський акцент. Схоже, це відео є частиною ширшої російської дезінформаційної кампанії, спрямованої на те, щоб показати погане керівництво, неадекватне командування, а також військові втрати та смерть в Україні.

В березні Росія поширювала твердження про те, що Радбез ООН «байдужий до страждань жителів Донбасу», через те, що Рада безпеки відмовилася пустити на засідання незаконно призначеного Росією «омбудсмена ДНР» (Морозова). У результаті пропагандисти почали поширювати новини про те, що Радбез ООН нібито «не вважає жителів Донбасу людьми». Центр стратегічних комунікацій вже розвінчав це неправдиве повідомлення. В ООН проголосували проти участі Морозової на засіданні через те, що російська влада незаконно призначила її «омбудсменом» тимчасово окупованих частин Донецької області. Офіційна українська влада не визнає цю «посаду» та пов'язаний з нею орган. У резолюції зазначалося, що запрошення на брифінг людини, яка нібито представляє Донецьк, є недоречним і спробою Росії опосередковано легітимізувати цю територію. Посол США в ООН Томас Грінфілд наголосив, що Росія несе відповідальність за катастрофічну гуманітарну ситуацію на тимчасово окупованих територіях України.

Два незалежних розслідування комісії ООН підтвердили вчинення Росією військових злочинів в Україні.

Також частиною Російської пропаганди є поширення у мережі відео про те, що в Луцьку та Рівному перепродують автомобілі, передані Україні як допомогу від Латвії. Твердження про те, що автомобілі, які продаються на відео, були конфісковані в Латвії, є неправдивими та не підтверджуються оригінальними кадрами. Це не перший випадок, коли пропагандисти поширюють неправдиву інформацію про те, що Україна перепродає допомогу від західних країн, і Росія використовує таку тактику, щоб підірвати довіру до міжнародних партнерів України [34].

Окрім Російсько-української війни, показовим прикладом того, як НАТО бореться з дезінформацією стала пандемія COVID-19. Як державні, так і недержавні суб'єкти використовували пандемію COVID-19 для поширення дезінформації та пропаганди, спрямованої на дестабілізацію та підрив західних суспільств. За останнє десятиліття низка державних суб'єктів, зокрема, розробила та впровадила методи цифрового маркетингу, доповнені як кібернетичними, так і психологічними операціями. Мета полягає в тому, щоб створити альтернативний світогляд, спрямований на підрив демократичних цінностей.

Контрольовані державою ЗМІ, такі як Russia Today (RT) і Sputnik, використовують новини, які містять як правдиві, так і неправдиві елементи, які обходять природні фільтри людей для виявлення дезінформації. Через організації, в тому числі петербурзьку «фабрику тролів» – офіційну назву – Агентство інтернет-досліджень – Росія використовує підроблені або автоматизовані облікові записи для поширення інформації, щоб розширити історію в соціальних мережах і на сайтах блогів [35].

У березні-червні 2020 року НАТО було об'єктом низки конкретних дезінформаційних атак, що збіглося з карантином через COVID-19 у багатьох членах НАТО. Лише за два дні (20-21 квітня) НАТО зафіксувало три скоординовані атаки на присутність військ НАТО в Латвії, Литві та Польщі. Ці атаки включали фальшивий лист нібито від генерального секретаря НАТО Єнса Столтенберга до

міністра оборони Литви Раймундаса Каробліса, в якому говорилося про намір НАТО вивести війська з країни, фальшиве інтерв'ю, в якому стверджувалося, що канадські війська в Латвії привезли вірус до країни, і підроблений лист польського воєначальника, який нібито критикує війська США.

У цей же період Росія поширювала неправдиві заяви про те, що НАТО продовжує проводити широкомасштабні навчання, не звертаючи уваги на обмеження поширення вірусу. Наприклад, Sputnik стверджував, що навчання НАТО Steel Brawler у Латвії піддасть ризику цивільне населення та збільшить кількість заражень COVID-19. Він зробив подібні заяви щодо морських навчань BALTOPS у Балтійському морі. Насправді Steel Brawler відбулися виключно на військових навчальних полігонах, спеціально для уникнення контакту з місцевим населенням, і BALTOPS відбувалися виключно в морі.

Навчання DEFENDER-Europe 20 під проводом США, під час яких тисячі американських військовослужбовців були розгорнуті в Європі, також були постійною мішенню дезінформації. Через пандемію навчання було зменшено за розміром і обсягом, але російські джерела продовжували стверджувати, що НАТО ігнорувало обмеження на подорожі та поширювало COVID-19 по Європі.

Щоб спростувати чутки щодо походження вірусу, офіційні китайські джерела спробували посіяти сумніви, навіть звинувативши союзників по НАТО в його спалаху. Китайський державний таблоїд Global Times у твіті припустив, що вірус міг виникнути в Італії, тоді як речник МЗС Китаю Чжао Ліцзянь написав у Твіттері, що армія США могла принести епідемію в Ухань [36].

Недержавні організації також намагалися використати пандемію у своїх повідомленнях. Терористичні групи або намагалися вербувати нових послідовників і влаштовувати напади, або покращити свій суспільний імідж. У своєму інформаційному бюлетені «Аль-Наба» терористичне угруповання ІДІЛ стверджує, що вчинення терористичних актів наділяє джихадистів імунітетом до COVID-19 і що його прихильники повинні скористатися цією можливістю для подальших атак. І ІДІЛ, і Аль-Каїда стверджують, що пандемія є проявом Божого гніву проти

«невірних». Аль-Каїда заохочує людей на Заході використати цей час для вивчення їхніх вчень і прийняття ісламу.

Ще одним прикладом дезінформації або інформаційної війни проти країн-членів членів НАТО є кампанія в Литві. У квітні 2020 року в рамках багатоетапної операції з дезінформації були поширені неправдиві заяви про те, що спалах COVID-19 у багатонаціональній бойовій групі НАТО в Литві призвів до рішення НАТО вивести свої війська. Фальшивий і оманливий контент новин був зосереджений на фальшивому листі від Секретаріату НАТО генерала Єнса Столтенберга до міністра оборони Литви Раймундаса Каробліса. Лист містив численні неправдиві ворожі наративи, пов'язані зі зростанням кількості інфекцій COVID-19 серед військ НАТО [35].

Мітки часу, пов'язані з операцією, вказують на те, що кампанія розпочалася з двох публікацій у блозі, однієї литовською та іншої англійською. Кожна версія містила різні неправдиві відомості про місцевий вплив COVID-19. Потім блоги поширювалися на низці новинних веб-сайтів і платформ соціальних медіа з використанням кількох одноразових підроблених облікових записів, у тому числі одного, який видавав себе за справжнього литовського журналіста. Облікові записи, які використовувалися, були здебільшого створені за кілька днів до публікації в блозі, що вказує на те, що операція була ретельно спланована.

Крім фальшивого листа та підтримуючих неавтентичних статей новин, операція також включала маніпульоване відео YouTube, яке реконтекстуалізувало прес-конференцію, що Генеральний секретар дав на зустрічі міністрів оборони НАТО 14 квітня 2020 року. Відео було змінено так, ніби конференція стосувалася виключно впливу COVID-19 на війська НАТО в Литві.

Потім фальшивий лист було надіслано електронною поштою безпосередньо до штаб-квартири НАТО за допомогою підробленої електронної адреси командування НАТО. Незважаючи на спроби імітувати офіційні повідомлення НАТО, електронний лист був низької якості та містив низку форматуючих, синтаксичних і граматичних помилок, які поставили його достовірність під сумнів.

Генеральний секретар НАТО Єнс Столтенберг сказав Baltic News Service: «Вони не досягли успіху, тому що, по-перше, було чітко виявлено, що це фальшивий лист; по-друге, ми побачили, що союзники по НАТО залишаються відданими, залишаються єдиними та фактично допомагають один одному в розпал коронавірусної кризи».

Незважаючи на чітке планування та координацію, кампанія не викликала значного інтересу в Інтернеті завдяки швидкій реакції Міністерства оборони Литви 20 та тісній співпраці з НАТО для розвінчання історії. Маргінальні блоги, новинні видання та публікації в соціальних мережах не викликали значного інтересу, ними поділилися менше 200 разів [36].

Наступний приклад дезінформації – лабораторії НАТО створили COVID-19. Російські державні ЗМІ та прокремлівські ЗМІ припустили, що латвійська лабораторія могла розробити коронавірус. Він також звинуватив у створенні COVID-19 «секретні лабораторії США/НАТО» в Грузії, Казахстані, Молдові та Україні. Перше російське припущення про те, що COVID-19 могло виникнути у військових лабораторіях США, з'явилося 20 січня 2020 року, приписане російському експерту, на телеканалі «Звезда 21», державному каналі, яким керує Міністерство оборони Росії.

27 січня підтримуваний Кремлем RenTV спробував покласти відповідальність за пандемію на Центр досліджень громадської охорони здоров'я Річарда Лугара в Тбілісі, американську біологічну лабораторію в Грузії. Росія продовжувала натякати, що США керують секретними лабораторіями в Грузії «в той час, коли світ має об'єднатися» [35].

Альянсу вдалось викрити і протидіяти всім цих фейкам завдяки системі комунікацій, яка базується на реальних діях і фактах. Ця система ґрунтується на основних цінностях Альянсу – демократії, свободі слова та верховенстві права. Залучення громадськості та підвищення стійкості в середньостроковій та довгостроковій перспективі є найефективнішим способом прищепити людей від дезінформації.

НАТО продовжуватиме викривати дезінформацію за допомогою широкого кола засобів масової інформації, включаючи заяви, спростування та виправлення, а також брифінги, щоб інформувати широку аудиторію про дезінформацію та пропаганду, як це було з часів до пандемії.

Щоб протистояти викликам поточної кризи і протидіяти фейкам і дезінформації, НАТО:

– посилює цифрові комунікації щодо протидії пандемії на всіх платформах. Поточну інформацію та новини, пов'язані з COVID-19, можна знайти на офіційному сайті.

– Щоб сформувати політичні дебати, НАТО перетворило заходи публічної дипломатії віч-на-віч на спілкування в Інтернеті.

– Покращило спілкування російською мовою: тобто розширило список матеріалів (статей, інформаційних бюлетнів і відео) для охоплення інформування ширшої території.

– НАТО підтримує роботу незалежних неурядових організацій, аналітичних центрів, науковців, організацій, що перевіряють факти, та інших ініціатив громадянського суспільства з метою сприяння діалогу і підвищення стійкості.

– Плюралістичний незалежний медіа-сектор також відіграє важливу роль у протидії дезінформації та донесенні до громадськості фактичної інформації. НАТО співпрацює зі ЗМІ, щоб надати своєчасну інформацію про свою відповідь на COVID-19 потенційній аудиторії в сотні мільйонів людей. НАТО провело брифінги для ЗМІ в багатьох країнах, включаючи Грузію, Молдову, Росію та Україну та регіон Західних Балкан, зосередивши увагу на дезінформації та внеску НАТО в боротьбу з COVID-19 [37].

Координація з партнерами та міжнародними інституціями лежить в основі напрямків «Зрозуміти» та «Залучати» у відповідь НАТО на дезінформацію. Щоб виявити, проаналізувати та протидіяти дезінформації, НАТО співпрацює з Європейським Союзом через Європейську службу зовнішньої дії та Європейську комісію, Механізм швидкого реагування G7, Організацію Об'єднаних Націй та її

перевірену кампанію та Глобальний центр взаємодії Державного департаменту США.

Отже, дезінформація, пропаганда та фейкові новини були проблемою протягом десятиліть, але особливо загострились під час глобальних викликів, таких як повномасштабне російське вторгнення в Україну і криза COVID-19. Пропагандистські наративи і неправдива інформація – це все сьогодні є новою зброєю масового ураження, яка може мати більший вплив на населення країн, ніж хімічна або біологічна, адже впливає на свідомість і думку людини. НАТО – як безпекова організація, що була створена з метою захисту країн-членів, сьогодні намагається убезпечити світ не лише від реальних фізичних загроз, але і від пропаганди і дезиінформації. І хоча поки єдиного механізму протидії дезинформації немає, але Альянс намагається співпрацювати з організаціями, урядами і населенням для виявлення фейкових новин і недопущення їх розповсюдження.

Як можна бачити, стратегічні комунікації є невід'ємною частиною зусиль щодо досягнення політичних і військових цілей Альянсу. НАТО є однією з найактивніших міжурядових інституцій у застосуванні стратегічних комунікацій як інструменту протидії дезінформації. Лише після глобальних викликів, таких як пандемія COVID-19 і російська агресія проти України, де Росія використовувала масштабні дезінформаційні кампанії для впливу на різні цілі (цивільне населення, українських військових, державних службовців, політиків тощо), НАТО по-справжньому усвідомила важливість інформаційних відповідей на гібридні загрози і неправдиву інформацію і фейки. НАТО намагається забезпечити здатність ефективно протистояти конкретним викликам, пов'язаним із загрозами дезінформації і налаштувати необхідні інструменти та процедури, необхідні для стримування та ефективного реагування на фейки і дезінформацію.

# РОЗДІЛ 3
# ПРОБЛЕМИ І ПЕРСПЕКТИВИ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ НАТО

## 3.1. Нові підходи Північноатлантичного Альянсу у сфері кібербезпеки в умовах загострення інформаційного протистояння

Зловмисна кіберактивність значно зросла за останні роки, особливо на тлі пандемії, а тепер і війни в Україні. Держави, недержавні суб'єкти та злочинні угруповання конкурують між собою та дедалі частіше використовують конфіденційну інформацію та проникають у мережі інших країн, щоб викрасти дані, ввести дезінформацію або порушити критичну інфраструктуру.

Пандемія коронавірусу стала поштовхом для ускладнення ландшафту кіберзагроз. У березні 2020 року спроби пом'якшити поширення коронавірусу призвели до заходів соціального дистанціювання, обмежень на подорожі та віддаленої роботи. За короткий проміжок часу фахівцям з IT-безпеки довелося реагувати на виклики, пов'язані з роботою з дому, наприклад, на переміщення корпоративних даних, коли співробітники отримували доступ до хмарних програм через домашній Інтернет, корпоративне програмне забезпечення, відеоконференції та обмін файлами. Навіть якщо існували апаратні та програмні рішення для захисту даних організації, часто не існувало встановлених політик, які б допомагали співробітникам пробиратися крізь джунглі загроз і вразливостей, з якими вони стикалися, переміщуючи своє робоче місце за межі традиційного офісного середовища.

Інший набір загроз приходить у формі войовничих державних акторів, які прагнуть викрасти конфіденційні дані для шпигунства. У грудні 2020 року російські спецслужби проникли в цифрові системи американської технологічної фірми SolarWinds і вставили в її код шкідливе програмне забезпечення. Під час наступного оновлення програмного забезпечення компанії вірус був випадково поширений приблизно на 18 000 клієнтів, включаючи великі корпорації, Пентагон, Державний

департамент, Міністерство фінансів та інші урядові установи США. Злом залишався непоміченим протягом кількох місяців, перш ніж жертви виявили, що величезну кількість їхніх даних було вкрадено [38].

З 2021 року український уряд почав зазнавати серії кібератак, які призвели до витоку інформації з урядових веб-сайтів і знищення даних на деяких державних комп'ютерах. У середині січня 2021 року хакери зламали близько 70 українських веб-сайтів, у тому числі міністерств закордонних справ, оборони, енергетики, освіти та науки, а також Державної служби з надзвичайних ситуацій та Міністерства цифрової трансформації. Міжнародний хакерський колектив Anonymous оголосив «кібервійну» проти російського уряду, взявши на себе відповідальність за кілька кіберінцидентів, включаючи розподілені атаки на відмову в обслуговуванні, які вивели з ладу російські урядові сайти та Росію.

Також у день російського вторгнення ViaSat, постачальник послуг високошвидкісного супутникового широкосмугового доступу, був зламаний разом з одним із його супутників Ka-Sat, користувачами якого були українські збройні сили, поліція та спецслужби [39].

Отже, ці приклади показують, що всьому світу застаріла критична інфраструктура вже давно є вразливою для атак в кіберпросторі. І щоб йти в ногу зі швидкими змінами ландшафту загроз і підтримувати надійний кіберзахист, НАТО прийняло розширену політику та план дій щодо кіберзахисту.

Взагалі за останні п'ятнадцять років підхід НАТО до кібернетичних проблем дещо покращився: члени перейшли від розгляду кіберзахисту, як, в першу чергу, технічних аспектів до розгляду його як важливої складової для стратегічного контексту альянсу. Необхідність «посилення спроможності та захисту від кібератак» вперше визнали лідери країн Альянсу на саміті 2002 року в Празі. Однак після того, як у 2007 році цифрова інфраструктура Естонії постраждала від кібератак, НАТО визнало, що протистояння між державами може включати кібервимір, і на Бухарестському саміті в 2008 році прийняло свою першу політику кіберзахисту.

Конфлікт 2008 року між Росією та Грузією продемонстрував, що кібератаки можуть стати головним компонентом звичайних бойових дій.

Паралельно Спільний центр передового досвіду кіберзахисту НАТО (CCDCOE) був акредитований як Центр передового досвіду НАТО у 2008 році. З того часу він перетворився на потужний міжнародний центр знань з кіберзахисту, який об'єднує найкращих кіберекспертів у різних сферах: урядові, військові, промислові та наукові кола – з 29 країн для міждисциплінарних досліджень, навчання у чотирьох основних сферах: технології, стратегія, операції та право. Центр об'єднує довірену спільноту країн-однодумців, які бажають поділитися інформацією та досвідом у сфері кібербезпеки. Найвідомішими проектами CCDCOE є «Locked Shields» – одні з найбільших і наймасштабніших у світі навчань з кіберзахисту; щорічна кіберконференція CyCon; і Талліннський посібник, який розглядає кібероперації в контексті міжнародного права [40].

На саміті в Уельсі 2014 року НАТО визнало, що міжнародне право застосовується в кіберпросторі, і заявило, що, оскільки наслідки кібератаки можуть бути такими ж шкідливими для сучасних суспільств, як і звичайні атаки, кіберзахист є частиною мандату НАТО щодо колективної оборони. Таким чином, НАТО визнало, що кіберпростір є операційною сферою для потенційних супротивників.

На саміті НАТО у Варшаві у 2016 році була прийнята декларація, в якій визнається, що кіберпростір перетворився на окрему сферу військових операцій, у якій альянс «повинен захищати себе так само ефективно, як і в повітрі, на суші та на морі» [41]. Подальша дорожня карта включала розробку доктрини кібероперацій НАТО, а також розвиток військових кіберспроможностей. У січні 2020 року було опубліковано Об'єднану доктрину Альянсу щодо операцій у кіберпросторі «для планування, виконання та оцінки операцій у кіберпросторі в контексті об'єднаних операцій Альянсу».

На саміті у Варшаві глави держав і урядів НАТО підписали зобов'язання щодо кіберзахисту, в якому вони окреслили, як країни захищають свої кібермережі. НАТО

розробила детальні анкети та показники, пов’язані з обіцянкою, і використовує їх для регулярного звітування про те, як кожна країна виконує свої кіберзобов’язання.

Під час саміту НАТО в липні 2018 року союзники вперше підтвердили свою рішучість «використовувати весь спектр можливостей, включаючи кібернетичні, для стримування, захисту та протидії повному спектру кіберзагроз», відійшовши від забезпечення безпеки кіберпростору. лише з оборонними заходами. «Повний спектр» кіберспроможностей означає, що НАТО може розгортати як оборонні, так і наступальні можливості відповідно до свого оборонного мандату та міжнародного права.

Наприкінці 2020 року група експертів, призначена генсеком НАТО Єнсом Столтенбергом під головуванням Томаса де Мезьєра з Німеччини та Веса Мітчелла зі Сполучених Штатів надали свої рекомендації щодо того, як НАТО може посилити свою політичну роль і краще координувати військові завдання та політичні стратегії між своїми членами.

На саміті в Брюсселі в 2021 році союзники схвалили нову Всеохоплюючу політику кіберзахисту, в якій наголошується на тому, що співпраця необхідна для міцного кіберзахисту, і в якій визнається, що «вплив значної зловмисної сукупної кіберактивності може, за певних обставин, розглядатися як збройна атака. Ключовою особливістю нової політики є видатна роль наступальних кібероперацій [42]. Іншими словами, альянс заявив, що може реагувати на зловмисну кіберактивність, яка не перевищує порогу застосування сили, що завдає значної шкоди, серед іншого, звичайними військовими або наступальними операціями в кіберпросторі.

НАТО розробило свою наступну Стратегічну концепцію до саміту 2022 року. По-перше, НАТО має переконати опонентів, що вони не можуть бути таємними у своїх кібер-діях. НАТО та його члени повинні продемонструвати, що важко або неможливо діяти таємно, і чітко визначити відповідальність за кібератаки.

Донедавна уряди публічно не оприлюднювали подробиці кіберінцидентів. Але з 2018 року публічне оприлюднення кібератак кількома західними державами свідчить про нову багатонаціональну політику прозорості держави. Ефективне публічне визначення вимагає чіткого розуміння відповідної кібероперації та суб'єкта кіберзагрози, а також ширшого геополітичного середовища, позицій і діяльності союзників, а також правового контексту. Збір і обробка розвідувальних даних – інформації про іноземні країни та їхніх агентів – забезпечує технічну основу для визначення авторства.

Як другий напрямок дій НАТО має використати поточну кризу, щоб прискорити прогрес у створенні власного кіберкомандування НАТО та посилити відповідь союзників на зловмисні кібер-акції.

Ці заходи мають відбуватись шляхом навчання, підвищення професіоналізму і кваліфікації кадрів, які працюють у сфері захисту кіберпростору. НАТО вже працює над цим і проводить регулярні навчання, такі як щорічні навчання Cyber Coalition Exercise, і має на меті інтегрувати елементи та міркування кіберзахисту в увесь спектр навчань Альянсу, включаючи навчання з управління кризовими ситуаціями (CMX). НАТО також розширює свої можливості для навчання, включно з кіберполігоном НАТО, який базується на об'єкті, наданому Естонією.

НАТО має низку практичних інструментів для покращення ситуаційної обізнаності та полегшення обміну інформацією, включаючи пункти контакту з національними органами кіберзахисту в кожній із 31 столиць Альянсу. Спеціальний Меморандум про взаєморозуміння (MOU) визначає механізми обміну різною інформацією, пов'язаною з кіберзахистом, і надання допомоги для покращення запобігання кіберінцидентам, стійкості та можливостей реагування. Технічна інформація також обмінюється через Платформу обміну інформацією про зловмисне програмне забезпечення НАТО, яка дозволяє кіберзахисникам Альянсу обмінюватися індикаторами компрометації [43].

Академія зв'язку та інформації НАТО (NCI) в Оейраші, Португалія, забезпечує підготовку персоналу країн-членів (а також країн, що не входять до НАТО) щодо експлуатації та обслуговування систем зв'язку та інформації НАТО. Академія NCI також пропонує навчання та курси з кіберзахисту.

Школа НАТО в Обераммергау, Німеччина, проводить освіту та навчання з кіберзахисту для підтримки операцій, стратегії, політики, доктрини та процедур Альянсу. Оборонний коледж НАТО в Римі, Італія, сприяє розвитку стратегічного мислення щодо військово-політичних питань, у тому числі питань кіберзахисту.

Третій захід спрямований на підвищення стійкості внутрішньої критичної інфраструктури. Усі країни-члени НАТО повинні вирішити свою цифрову незахищеність, заблокувавши цифрові «двері» як окремим особам, так і компаніям та країнам. Стратегічна вразливість до збоїв і диверсій полягає не стільки у військовому просторі, скільки в системі бронювання госпіталів, розкладі логістики, електромережі та тисячах інших основних, цивільних, переважно приватних мереж. Це також включає зміцнення політичної стійкості держав-членів шляхом розширення консультацій НАТО з охопленням більшої кількості сфер управління. Регулярні зустрічі у форматі Північноатлантичної ради між керівниками кіберорганів держав-членів на політичному та військовому рівнях допоможуть досягти консенсусу щодо питань кіберполітики.

Іншим напрямком дій НАТО в галузі кібербезпеки є посилення зусиль із розбудови кіберпотенціалу для країн-партнерів, які мають стратегічне значення, зміцнюючи прихильність НАТО і створюючи стабільність у сусідстві з НАТО. Такий вид розбудови кіберпотенціалу може включати різні типи підтримки, починаючи від стратегічних консультацій і розбудови кіберінституцій у секторах оборони до освіти та навчання або консультацій і допомоги в кіберзахисті. Кіберзахист є однією зі сфер посилення співпраці між НАТО та ЄС у рамках все більш скоординованих зусиль двох організацій із протидії гібридним загрозам. НАТО та ЄС обмінюються інформацією між групами кіберреагування та

обмінюються передовим досвідом. Також розширюється співпраця щодо навчання, досліджень і навчань із відчутними результатами у протидії кіберзагрозам.

Приватний сектор є ключовим гравцем у кіберпросторі, а технологічні інновації та досвід приватного сектору мають вирішальне значення для того, щоб НАТО та країни Альянсу могли ефективно реагувати на кіберзагрози.

Завдяки Промисловому кібер-партнерству НАТО (NICP) НАТО та його союзники працюють над зміцненням своїх відносин із промисловістю та науковими колами. Це партнерство включає організації НАТО, національні групи реагування на комп'ютерні надзвичайні ситуації (CERT) і представників промисловості членів Альянсу. Обмін інформацією, навчання, підготовка та освіта – це лише кілька прикладів сфер, у яких НАТО та промисловість співпрацюють [44].

Отже, загалом, більшість майбутніх конфліктів матимуть кіберкомпоненти, які потребуватимуть технічної, політичної та дипломатичної відповіді. Незалежно від того, чи є супротивник елітним підрозділом держави чи злочинним угрупуванням, яке надає програмне забезпечення як послугу, кібербезпека полягає в управлінні ризиками та надійному, прагматичному з ахисті та заходах реагування для підвищення безпеки цифрового середовища. В сучасних умовах (де основною загрозою наразі для світової спільноти залишається Росія) враховучи непередбачуваність режиму Путіна, ризик ескалації ворожих кіберобмінів між Росією та країнами НАТО залишається високим. Зрозуміло лише те, що станом на 24 лютого 2022 року ми живемо в іншому світі, в якому європейський і світовий порядок безпеки зруйновано. Тому тепер державам-членам Альянсу належить забезпечити ясність і узгодженість, щоб успішно розробити нову Стратегічну концепцію, яка включає оборону та стримування кіберзагроз. Але це робота не лише для НАТО – вона вимагає тісної координації між національними урядами та приватним сектором, і тому НАТО та Європейський Союз повинні продовжувати дуже тісно співпрацювати над цим життєво важливим питанням.

### 3.2. Діджиталізація процесів публічної комунікації як один із пріоритетних напрямків інформаційної політики НАТО

Такі технології, як великі дані, штучний інтелект (ШІ), автономні системи та квантові технології, змінюють світ і те, як працює НАТО. Ці та інші нові та революційні технології (EDT) створюють як ризики, так і можливості для НАТО та членів Альянсу. Ось чому Альянс співпрацює з партнерами з державного та приватного секторів, науковими колами та громадянським суспільством над розробкою та впровадженням нових технологій, встановленням міжнародних принципів відповідального використання та підтриманням технологічної переваги НАТО.

Цифровізація може посилити здатність НАТО збирати та обробляти інформацію, приймати рішення та автоматизувати рутинні процеси. Розширення масштабів, властиве цифровізації, дозволяє НАТО консолідувати вхідні дані в низці секторів для кращої обізнаності про ситуацію, навіть у сферах, які виходять за рамки традиційної регіональної та функціональної експертизи. Альянс має чіткі структури прийняття рішень і командування зі встановленими лініями повноважень і чітко визначеними процесами. Кожну стадію процесу прийняття рішень НАТО можна покращити, оскільки цифровізація дає змогу Альянсу зміцнити свою позицію стримування та оборони та вдосконалити важливі сфери в епоху цифрових технологій: перемогти як опортуністичні, так і скоординовані кампанії дезінформації, прогнозувати стратегічні потрясіння.

Цифровізація і діджиталізація стали основними пунктами в новій концепції НАТО, прийнятій на саміті в Мадриді в 2022 році і, яка визначає цілі і пріоритети розвитку організації наступні роки. Стратегічна концепція є одним з найважливіших документів НАТО, оскільки вона дає інформацію для планування подальших дій альянсу, розподілу ресурсів і програмування на основі змін у середовищі загроз. Але документ не оновлювався з 2010 року. Стратегічна концепція 2010 року під назвою «Активне залучення, сучасна оборона» містила лише одне коротке речення про

кібератаки. У ньому також зазначено, що «сьогодні в євроатлантичному регіоні панує мир», незважаючи на те, що Росія вторглася в Грузію за два роки до цього, і нависла загроза повернення до конкуренції великих держав [45].

Анексія Росією Криму та інтервенція на Донбасі в 2014 році та вторгнення в Україну в 2022 році зруйнували будь-які ілюзії тривалого миру з Росією. Територіальні амбіції Китаю, економічна самовпевненість, загрози Тайваню та військова модернізація загрожують порядку, заснованому на правилах. Нові технології – у формі гіперзвукової зброї, штучного інтелекту, квантових обчислень і машинного навчання – посилили конкуренцію за першість на світовій арені.

Стратегічна концепція 2022 року підкреслює важливу роль технологій у колективній обороні. Щоб створити більший цифровий потенціал і водночас підкреслити стійкість, НАТО має прийняти нову технологічну орієнтацію на військово-стратегічному рівні командування, особливо в рамках Об'єднаного командування з питань трансформації (АСТ) у Норфолку, штаті Вірджинія, та Командування об'єднаних збройних сил НАТО з операцій (АСО) у Монсі, Бельгія. АСТ використовує передові технології для безпеки та оборони в можливостях, процедурах, державно-приватних партнерствах, цивільно-військових відносинах і в Центрах передового досвіду НАТО.

За рік до саміту в Мадриді (в 2021 році) в рамках порядку денного НАТО до 2030 року лідери країн Альянсу погодилися запустити Інноваційний прискорювач оборони в Північній Атлантиці (DIANA) і створити міжнаціональний фонд венчурного капіталу для підтримки інновацій в Альянсі.

Через рік, на саміті НАТО в Мадриді у 2022 році, усі лідери Альянсу схвалили хартію для DIANA та оприлюднили її початкові центри випробувань і прискорювачі. Окремо лідери 22 країн-членів Альянсу взяли на себе зобов'язання взяти участь у Інноваційному фонді НАТО вартістю 1 млрд євро, першому у світі мультисуверенному фонді венчурного капіталу, який розпочне свої інвестиції у 2023 році.

DIANA – це новий орган НАТО, який працює безпосередньо з провідними підприємцями, від молодих компаній-початківців до більш зрілих компаній, для вирішення критичних проблем у сфері оборони та безпеки за допомогою глибоких технологій (тобто трансформаційних технологій, які вирішують важливі виклики через конвергенцію прориву) науки та техніки [46].

DIANA запустить конкурсні програми Challenge. Кожна програма Challenge базуватиметься на критичних проблемах оборони та безпеки та буде спрямована на сприяння найефективнішим технологічним рішенням, розробленим найкращими та найталановитішими новаторами з усього Альянсу. Новатори, прийняті в DIANA, отримають доступ до мережі з понад дев'яти сайтів Accelerator і 63 тестових центрів в інноваційних центрах по всьому Альянсу, а також отримають нерозбавлене фінансування (тобто інвестиційний капітал, який не вимагає від них відмови від власного капіталу або право власності на свою компанію). Вони також отримають доступ до мережі надійних інвесторів вищого рівня, бізнес-наставництва та навчання від експертного персоналу DIANA, найсучасніших можливостей для тестування та можливості для розробки та впровадження контрактів із членами Альянсу щодо запропонованих технологій подвійного використання.

DIANA розпочне пілотну діяльність уже влітку 2023 року. Після повного запуску в 2025 році вона матиме можливість взаємодіяти з сотнями інноваторів щороку через ще більш широку мережу сайтів прискорювачів і тестових центрів по всьому Альянсу.

Лідери НАТО також домовилися на Брюссельському саміті 2021 року створити Фонд інновацій НАТО. Фонд венчурного капіталу в розмірі 1 млрд євро забезпечить стратегічні інвестиції в стартапи, що розробляють нові та революційні технології подвійного призначення в сферах, які мають вирішальне значення для безпеки Альянсу [47]. Фонд стане першим у світі мультисуверенним фондом венчурного капіталу.

Багато стартапів, які працюють над технологіями, намагаються залучити достатні інвестиції через тривалий час виходу на ринок і високу капіталомісткість їхніх досліджень. Інноваційний фонд НАТО вирішить цю проблему, використовуючи свою унікальну позицію терплячого інвестора з 15-річним періодом роботи, який краще підходить для розширених часових горизонтів, необхідних для стартапів технологій. Кошти будуть видаватись проектам і розробкам, які відповідатимуть трьом стратегічним цілям Фонду:

– шукати передові технологічні рішення, які вирішують проблеми оборони та безпеки Альянсу;

– зміцнювати глибокотехнологічні інноваційні екосистеми в Альянсі; і

– для підтримки комерційного успіху свого портфоліо глибокотехнологічних стартапів [47].

На саміті НАТО в Мадриді 2022 року Фонд завершив свій список країн-учасниць, і лідери 22 країн-членів Альянсу підписали лист про зобов'язання: Бельгія, Болгарія, Чехія, Данія, Естонія, Німеччина, Греція, Угорщина, Ісландія, Італія, Латвія, Литва, Люксембург, Нідерланди, Норвегія, Польща, Португалія, Румунія, Словаччина, Іспанія, Туреччина та Великобританія. Зараз фонд знаходиться в процесі формування та розпочне початкові інвестиції у 2023 році.

Стратегічна концепція 2022 заохочує співпрацю у впровадженні керівних принципів і процедур через концепцію «Plug-and-play», за якою платформи та системи оптимізовані для готовності та реагування з блискавичною швидкістю. Plug-and-play базується на підходах, які використовуються в комерційному програмному забезпеченні, які дозволяють інноваційний та легкий доступ до мереж і систем через безпечні платформи. Наприклад, Платформа НАТО для обміну інформацією про стрілецьку зброю та легке озброєння (SALW) і протимінну діяльність (МА) містить численні та загальнодоступні набори даних про роль, яку відіграє Альянс у боротьбі з незаконною торгівлею стрілецькою зброєю, танками, літаками та морськими кораблями. Він звітує та оновлює проекти, що фінансуються

НАТО, щоб запобігти придбанню супротивниками цієї зброї. Однак платформа SALW-MA застаріла та незручна для користувача, що перешкоджає її функціональності на практиці [48].

Простіше кажучи, АСТ і АСО НАТО повинні зосереджуватися на полегшенні доступу до інформації так само, як і на передових технологіях і звичайному озброєнні. Це надасть НАТО корисні інструменти для доступу до даних і розвідданих на стратегічному, оперативному та тактичному рівнях, а також у наземних, морських, повітряних, космічних та кібернетичних сферах за допомогою пристроїв і платформ, які можуть безперебійно підключатися один до одного і до баз даних в різних місцях. Але командування НАТО не може просто очікувати, що наявний персонал пристосується. Їх необхідно регулярно навчати використовувати цифрову інфраструктуру таким чином, щоб полегшити їхню роботу.

Спеціалісти зі стратегічного планування, кібероператори та бійці НАТО повинні пройти підготовку та навчання щодо відповідних цифрових платформ, доступу та обміну даними й інформацією таким чином, щоб покращити спільне прийняття рішень і колективну оборону.

У Стратегічній концепції 2022 року підкреслюється зв’язок між державами-членами в багатодоменних операціях і у співпраці з приватним сектором і академічними колами. Завдання для НАТО полягає в тому, щоб АСТ і АСО підвищили доступність цифрових платформ і полегшили зв’язок між платформами. Тут штучний інтелект (ШІ) може зіграти роль у подоланні критичних перешкод.

Зараз ШІ займає більше місця в орієнтації колективної оборони НАТО. Завдання Стратегічної концепції 2022 року полягає у визначенні ступеня, до якого ШІ покращить здатність альянсу аналізувати інформацію та оцінювати дані: штучний інтелект допоможе військовому та цивільному персоналу НАТО взаємодіяти між пристроями на різних платформах, проводити ретельний аналіз даних і прискорювати час реакції у відповідь на звичайну або гібридну атаку.

У жовтні 2022 року міністри оборони країн НАТО домовилися про створення Експертної ради для управління відповідальною розробкою та використанням штучного інтелекту та даних у рамках всієї організації. Першим завданням ради стане розробка зручного для користувачів стандарту сертифікації відповідального ШІ, включаючи контроль якості та зниження ризиків, який допоможе привести нові проекти в галузі ШІ та даних у відповідність до Принципів відповідального використання, затверджених НАТО у жовтні 2021 року. Рада також буде унікальною платформою для обміну передовим досвідом, орієнтувати інноваторів та кінцевих користувачів на етапі розробки, сприяючи тим самим зміцненню довіри в інноваційній спільноті. В даний час НАТО тестує використання ШІ в різних галузях, як кіберзахист, зміна клімату та аналіз зображень [49].

У відповідь на заклик Стратегічної концепції 2022 року прискорити цифрову трансформацію члени НАТО також схвалили першу концепцію цифрової трансформації НАТО. До 2030 року цифрова трансформація НАТО дозволить Альянсу проводити операції в різних сферах, забезпечувати оперативну сумісність у всіх сферах, підвищувати обізнаність щодо ситуації, а також полегшувати політичні консультації та прийняття рішень на основі даних.

Зусилля НАТО в галузі нових та новітніх технологій, стратегія НАТО в галузі штучного інтелекту та рамкова політика НАТО щодо використання даних сприятимуть втіленню цього бачення в життя. Додаткові кроки були зроблені завдяки затвердженню міністрами оборони пріоритетних областей застосування передового аналізу даних, у тому числі для забезпечення операцій у різних сферах та підвищення обізнаності про обстановку, а також прийняття першого плану НАТО з реалізації автономних систем.

ШІ, експлуатація даних та автономні системи входять до дев'яти пріоритетних для НАТО технологічних областей. До них також належать: квантові технології, біотехнології та покращення людського потенціалу, гіперзвукові технології, нові матеріали та виробництво, енергетика та рухові установки, а також космос.

Існуюче партнерство, яке довело ефективність, – це співпраця НАТО з Klarrio, фірмою, яка надає Альянсу інноваційні послуги аналізу даних у реальному часі та потокові послуги для боротьби з дезінформацією та фейковими новинами. Klarrio співпрацює з Центром стратегічних комунікацій НАТО (StratCom), щоб допомогти Альянсу в інформаційній сфері шляхом потокового аналізу даних, обробки та аналітики програм для виявлення та викорінення дезінформації для планувальників стратегічного рівня НАТО. Він підтримує та оновлює служби панелі керування для відстеження підозрілих дій на платформах соціальних мереж, підтримує інтерактивний інтерфейс користувача, створює аналітичні звіти та використовує машинне навчання для аналізу даних та інформації [50].

Отже, для ведення війни на полі бою НАТО все ще потребуватиме вдосконалених авіаносців і танків. Однак НАТО також потребує цифрових інструментів, які дозволять його бійцям легко отримувати доступ до інформації та даних у сучасному бойовому просторі. Тоді як «поля битв» виділяють наземні операції над іншими, «простори битв» не пов’язані з конкретною ареною. Доступ до даних та інформації є необхідною умовою для обізнаності про ситуацію в різних областях.

Стримування гібридних атак у формі кібер-вторгнень, дезінформації через платформи соціальних мереж або зловмисних операцій впливу вимагає від НАТО захисту своєї цифрової інфраструктури та забезпечення більшого доступу до інформації та даних. Підхід усього Альянсу, заснований на багатонаціональній співпраці та координації та зосереджений на цифровій доступності, посилить стійкість НАТО.

### 3.3. Стан і перспективи інформаційної діяльності НАТО щодо євроатлантичної інтеграції України

Гібридна агресія Російської Федерації проти України створила нові загрози для держав-членів НАТО, що вимагало посилення співпраці між НАТО та Україною, особливо у невійськових сферах, серед яких і діяльність в сфері стратегічної комунікації. У таких умовах Україна потребує більшої допомоги з боку Альянсу; однак вона сама вже стала джерелом знань і досвіду ведення гібридної війни. Взагалі активна співпраця України з НАТО розпочалась в 2016 році шляхом поєднання Центру інформації та документації НАТО (1997 р.) та Офісу зв'язку НАТО (1999 р.).

Сьогодні така співпраця фактично перетворюється на спільне реагування на гібридні загрози, яке має надалі зосереджуватися на таких ключових невійськових сферах, зокрема:

- протидія надзвичайним ситуаціям;
- науково-технічне співробітництво;
- міжпарламентська співпраця;
- політичне співробітництво;
- протидія кіберзагрозам;
- енергетична безпека;
- розвиток цивільного персоналу у сфері безпеки;
- розвиток цінностей демократії, свободи особистості та верховенства права тощо [51].

Після Варшавського саміту НАТО в липні 2016 року практична допомога НАТО Україні надавалася у формі Комплексного пакету допомоги (CAP) Україні. У 2016 році StratCom Ukraine у співпраці з Центром інформації та документації НАТО, Міністерством оборони Великої Британії, Міністерством інформаційної політики, РНБО, іноземними та українськими експертами розробили концепцію побудови

системи урядових стратегічних комунікацій, яка стала основою Національної Доктрина інформаційної безпеки.

Починаючи з 2016 року, НАТО співпрацює з відділом публічної дипломатії МЗС, забезпечуючи стратегічне планування та допомагаючи йому в щоденній комунікаційній діяльності. Також НАТО продовжує пілотувати Production Hub – український підрозділ StratCom, який створює контент для державних установ. За два роки він підготував понад 40 кампаній для українських державних установ.

У 2017 році спільно з Національним інститутом стратегічних досліджень НАТО провело аудит системи кризових комунікацій в органах державної влади та розпочали розбудову державної системи кризових комунікацій.

У червні 2017 року Верховна Рада України (Верховна Рада України) прийняла закон, визначення членства країни в Альянсі як стратегічного пріоритету національної зовнішньої та безпекової політики. У 2019 році набула чинності відповідна зміна до Конституції України; у вересні 2020 року Президент України Володимир Зеленський заявив про готовність надати нового імпульсу розвитку відносин між Україною та НАТО та схвалив нову Стратегію національної безпеки України; з 12 червня 2020 року Україна є однією з шість країн зі статусом партнера НАТО в рамках Ініціативи взаємодії партнерства (PII) [52].

На фоні агресивних дій Росії проти України – не лише незаконної анексії Криму, а й використання кібератак, дезінформації та інших гібридних дій – на саміті НАТО у Варшаві було створено Платформу Україна-НАТО з протидії гібридній війні. Вона надає механізм для кращого виявлення гібридних загроз і нарощування спроможності у визначенні вразливостей і посиленні стійкості держави та суспільства. Тривають проекти на підтримку досліджень, навчання та експертних консультацій, зосереджені на отриманих уроках, протидії дезінформації та підвищенні стійкості.

Після незаконної анексії Росією Криму та дестабілізації східної України в 2014 році експерти НАТО надавали поради щодо планів України на випадок

надзвичайних ситуацій і заходів врегулювання кризових ситуацій для захисту критичної енергетичної інфраструктури та захисту цивільного населення. Сьогодні співпраця зосереджена на покращенні національного потенціалу громадянської готовності та стійкості. У 2019 році Група консультативної підтримки стійкості (RAST) підготувала рекомендації українським установам щодо посилення національної стійкості. На прохання України на початку 2022 року, перед повномасштабним вторгненням Росії відбулися подальші консультації RAST на рівні експертів, які надавали технічні поради для підтримки довгострокової стійкості країни та заходів цивільної готовності. Україна також регулярно бере участь у заходах, організованих Євроатлантичним центром координації реагування на катастрофи НАТО, і сама приймала численні навчання з реагування на катастрофи [53].

Наступна програма співпраці в сфері стратегічних комунікацій – «Партнерство заради миру» (ПЗМ). Участь у Процесі планування та перегляду ПЗМ допомогла Україні встановити та досягти амбітних, але реалістичних цілей щодо реформ оборони та безпеки, трансформації та розвитку потенціалу; для покращення здатності своїх сил діяти разом із силами Альянсу та партнерів у реагуванні на кризи та операціях з підтримки миру; а також для посилення спроможності України приймати сили Альянсу та партнерів для навчань і тренувань.

Також з 2007 року Україна бере участь в Ініціативі НАТО з розбудови доброчесності, яка надає практичну допомогу та поради для зміцнення доброчесності, підзвітності та прозорості в секторі оборони та безпеки. У жовтні 2019 року дев’ять інституцій сектору оборони та безпеки України завершили процес самооцінки та експертної оцінки НАТО BI, який забезпечив ретельну оцінку інституційних потреб і вразливостей і запропонував набір галузевих рекомендацій на рівні політики для покращення ефективного управління та подальшої роботи. стійкі антикорупційні реформи в оборонному секторі та суміжних секторах безпеки. Виходячи з цього, спеціальна програма заходів продовжує надавати два рівні підтримки з розбудови спроможності – спеціальну експертизу для інституцій для

покращення належного управління та управління оборонними ресурсами (фінансовими, людськими та матеріальними), а також освітню та навчальну діяльність для розвитку індивідуальних здібностей та сприяння організаційній культурі доброчесності.

Ще одна програма – програма вдосконалення оборонної освіти (DEEP) допомогла покращити та реструктуризувати системи військової освіти та професійної підготовки в Україні, зосередившись на восьми вищих навчальних закладах військового профілю та п’яти навчальних центрах для сержантського складу. Крім того, DEEP консультує керівництво академіями та університетами, підтримує викладачів у тому, як викладати, і допомагає в розробці курсів з лідерства та процесів прийняття рішень.

Напередодні цих програм, Україна в 2006 році приєдналась до ще однієї ініціативи НАТО – Програми обміну даними про повітряну обстановку. Вона покращує обізнаність та авіаційну безпеку шляхом взаємного обміну даними про повітряну обстановку, що покращує оперативну ефективність протиповітряної оборони шляхом ідентифікації, класифікації та потенційного усунення конфліктів повітряних суден. Цей потенціал мав особливу оперативну актуальність і користь після подальшого вторгнення Росії на українську територію з лютого 2022 року. НАТО тісно співпрацює з Україною, щоб надати якомога релевантнішу інформацію.

Наразі Україна розробляє спільно з НАТО Робочий план Військового комітету, який зосереджується на покращенні оперативної сумісності та оперативних можливостей збройних сил України, а також робить суттєвий внесок у поточні реформи безпеки та оборони. Також Україна бере активну участь в Програмі оцінки та зворотнього зв’язку Концепції оперативних можливостей яка підтримує подальший розвиток збройних сил, а також дає змогу Альянсу формувати спеціалізовані пакети сил, які можна розгортати на підтримку операцій і місій під проводом НАТО [54].

Додатково до вищеперерахованих програм, Україна бере активну участь у програмі НАТО «Наука заради миру та безпеки» (SPS) з 1991 року. Спільна робоча група з наукового та екологічного співробітництва сприяє визначенню пріоритетних сфер практичного наукового співробітництва в рамках програми SPS. З 2014 року, у відповідь на кризу в Україні, співробітництво у сфері цивільної науки та технологій, пов'язаних із безпекою, було посилено, і Україна стала найбільшим бенефіціаром Програми SPS. Провідні сфери співпраці з Україною в рамках SPS включають передові технології, боротьбу з тероризмом, захист від хімічних, біологічних, радіологічних і ядерних агентів, а також енергетичну та екологічну безпеку. Серед цих заходів варто відзначити участь України в програмі DEXTER, яка розробляє інтегровану систему виявлення вибухівки та вогнепальної зброї в громадських місцях.

Крім перерахованих вище програм, Україна брала участь у багатьох інших ініціативах, організованих консультативною місією Представництва НАТО в Україні. НАТО підтримує Україну у виконанні Резолюції Ради Безпеки ООН 1325 щодо жінок, миру та безпеки. Було створено законодавчу базу, яка дала змогу НАТО та Україні далі розвивати оперативну співпрацю, включаючи Угоду про статус збройних сил у рамках програми «Партнерство заради миру» (ПЗМ) (набула чинності у травні 2000 р.); Угода про підтримку приймаючої країни (ратифікована в березні 2004 р.); та Угода про стратегічні авіаперевезення (ратифікована в жовтні 2006 р.).

У червні 2020 року Україна стала партнером розширених можливостей (ЕОР). Цей статус надається учасникам Ініціативи партнерської сумісності НАТО, які зробили особливо значний внесок в операції НАТО та інші цілі Альянсу. Статус ЕОР працює як фасилітатор, надаючи Україні преференційний доступ до інструментарію оперативної сумісності НАТО, включаючи навчання, обмін інформацією та обізнаність про ситуацію. Україна також розширила спроможність і оперативну сумісність завдяки участі в Силах реагування НАТО [55].

Співпраця між НАТО та Україною у сфері реформування сектора оборони та безпеки є більш широкою, ніж з будь-якою іншою країною-партнером. Спільна робоча група Україна-НАТО з питань оборонної реформи (JWGDR) є основним напрямком співпраці у цій сфері. Створена у 1998 році під егідою Комісії Україна-НАТО, JWGDR здійснює ініціативи у сфері цивільно-військових відносин, демократичного контролю та цивільного управління збройними силами та іншими відомствами сектору безпеки, оборонного планування, розробки політики, стратегії та концепції національної безпеки. JWGDR дозволяє Україні використовувати значний досвід і знання країн Альянсу та служить інструментом, за допомогою якого Альянс може спрямувати допомогу. Він також забезпечує інституційну основу для співпраці НАТО з міністерствами та відомствами, які займаються впровадженням реформи сектору оборони та безпеки в Україні. До них належать РНБО, міністерства закордонних справ і оборони, Національна гвардія, Прикордонна служба, Служба безпеки України, Верховна Рада та інші.

З 2004 року Спільна робоча група Україна-НАТО з оборонно-технічного співробітництва працювала над посиленням співпраці у розвитку спроможності, процесах закупівлі оборонного обладнання та розробці технічних стандартів. Це включає стандартизацію, кодифікацію, матеріально-технічне забезпечення та управління життєвим циклом, а також співпрацю з Конференцією національних керівників озброєнь НАТО та Науково-технологічною організацією НАТО.

Отже, З 2014 року, після незаконної анексії Криму Росією, співпраця України з НАТО активізувалась у критичних сферах. З моменту повномасштабного вторгнення Росії в Україну, яке розпочалося в лютому 2022 року, НАТО та країни Альянсу надали Україні безпрецедентний рівень підтримки. Але підтримка України з боку НАТО та діяльність у партнерстві з країною почалися не в 2014 чи 2022 роках – практична співпраця між НАТО та Україною триває з 1990-х років. Протягом багатьох років співпраця України з НАТО була взаємовигідною та охоплювала широкий спектр заходів – від розбудови спроможностей України до

підтримки невійськових заходів, таких як співпраця в сфері наукових досліджень, сфері стратегічних комунікацій та публічної дипломатії.

# ВИСНОВКИ

Стратегічні комунікації є важливою складовою діяльності НАТО, оскільки, з одного боку, дозволяють забезпечувати ефективне спілкування з широкою аудиторією та формувати довіру та підтримку громадськості щодо місії та цілей організації, з іншого боку, стратегічні комунікації є одним із проявів влади організації та є інструментом у політико-безпековій реалізації інтересів Альянсу. У контексті сучасних конфліктів це вираження гібридної дії, яка може мати наступальний і оборонний характер. Головна мета – вплинути на громадську думку з метою зміни ставлення до культурних і політичних цінностей.

Однією з основних функцій стратегічних комунікацій в НАТО є забезпечення широкого розуміння внутрішніх процесів, прийнятих рішень та стратегічних дій НАТО. Це досягається через проведення різноманітних комунікаційних заходів, таких як прес-конференції, брифінги для журналістів, вебінари, інформаційні бюлетені та інші.

Крім того, стратегічні комунікації також мають на меті забезпечити ефективну взаємодію з партнерами та союзниками НАТО. Це досягається шляхом встановлення контактів, проведення консультацій та обміну інформацією.

НАТО також активно використовує соціальні медіа для забезпечення взаємодії зі широкою громадськістю. Це включає в себе використання Twitter, Facebook та інших платформ для поширення інформації, а також для відповіді на запитання та коментарі. Усі ці заходи спрямовані на забезпечення ефективного спілкування з різними аудиторіями, зокрема з медіа, громадськістю та партнерами, і забезпечення підтримки місії та цілей НАТО.

Діджиталізація і цифровізація, як глобальні процеси, що відбуваються сьогодні на всіх рівнях міжнародної діяльності, повністю змінюють порядок денний функціонування організацій і діяльності інших акторів світової арени. І чим більше покладатись на кібер-можливості, які пропонує кіберпростір, тим більше потрібно враховувати нові типи загроз, які можуть суттєво вплинути на повсякденну діяльність, роботу критичної інфраструктури та доступ до різноманітних послуг.

Щоб захистити та захистити кіберпростор і життєво важливу інформаційну інфраструктуру, Альянс має власну політику та стратегію кібербезпеки. Сьогодні НАТО та його країни-члени розглядають кібербезпеку та кіберзахист як пріоритетну сферу. У 2016 році було прийнято важливе рішення в історії Альянсу, коли НАТО оголосила про визнання кіберпростору зоною операцій. З того часу заходи НАТО з захисту кіберпростору країн-членів включають: розробку стратегічних документів та політик в галузі кібербезпеки, які визначають загальні принципи та підходи до кібербезпеки НАТО та її членів; взаємодію з країнами-членами НАТО та іншими країнами для обміну досвідом та інформацією щодо кібербезпеки; розвиток кібероборонної інфраструктури, включаючи створення центрів кібербезпеки та проведення тренінгів; розробку та впровадження технологічних рішень для захисту від кіберзагроз та виявлення кібератак; співпрацю з приватним сектором та академічними закладами з метою вдосконалення кібербезпеки.

В нестабільний і важкий для України час, для неї є дуже важливою співпраця з НАТО, яка б включала не лише військову допомогу, але і інші види, серед яких співпраця в галузі стратегічних комунікацій. Співпраця України з НАТО в галузі стратегічних комунікацій є дуже важливою, оскільки допомагає Україні забезпечити ефективність своїх комунікацій з міжнародним співтовариством, зокрема з країнами-членами НАТО, а також після 2014 року і особливо після лютого 2022 року, співпраця з НАТО допомагає доносити правдиву інформацію світовим лідерам, висвітлювати події Російсько-української війни, розповсюджувати правильні наративи і давати відсіч російській агресії не лише на фізичному полі бою, а й в кіберпросторі.

Саме завдяки співробітництву з НАТО, Україна отримує необхідну інформацію і вдало використовує її для перемог на фронті. Україна вже є учасником різноманітних програм, серед яких «Партнерство заради миру», Платформа «Україна-НАТО з протидії гібридній війні», Ініціатива НАТО з розбудови доброчесності. Україна й надалі отримуватиме рішучу політичну та практичну підтримку НАТО.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Щава К.О. Механізми публічної дипломатії // Матеріали Всесвітньої науково-практичної конференції з міжнародною участю «Дипломатія в міжнародних відносинах: ретроспекція і сучасність». 2023. С. 115-117.
2. Щава К.О. Наслідки російсько-української війни для НАТО // Матеріали XVI Міжнародної науково-технічної конференції «АВІА-2023». 2023. С. 27.50-27.52.
3. Щава К.О. Стратегічна комунікаційна діяльність НАТО у відповідь на вторгнення Росії на територію України // Тези доповідей / XXIII Міжнародної науково-практичної конференції здобувачів вищої освіти і молодих учених «Політ». 2023. С. 170-172.
4. Zerfass, Ansgar, et al Strategic communication: Defining the field and its contribution to research and practice // International Journal of Strategic Communication. 2018. Vol. 12.4. P. 487-505.
5. Falkheimer, Jesper, and Mats Heide // Strategic communication: An introduction to theory and global practice // Taylor & Francis. 2022.
6. Werder, Kelly Page, et al // Strategic communication as an emerging interdisciplinary paradigm // International Journal of Strategic Communication. Vol. 12.4.2018. P.333-351.
7. Любарець, Д. М. // Нові підходи НАТО до стратегічних комунікацій з 2014 року // Міжнародні відносини та міжнародне право в постбіполярній системі. 2023. С.101.
8. Олійник, А. // Форми, види, способи здійснення стратегічних комунікацій // Редакційна колегія: АМ Черняк, доктор юридичних наук, професор; ОВ Акульшин; ЛФ Компанцева. 149 с.
9. Merlingen, Michael // Coloniality and the Global North war against disinformation: the case of the European Union // Third World Quarterly. 2022. P. 1-18.
10. Svetoka, Sanda // Social media as a tool of hybrid warfare // NATO Strategic Communications Centre of Excellence, 2016.

11. Ільницька, Уляна Вікторівна // Інформаційно-комунікативна політика НАТО та практика реалізації стратегічних комунікацій Північноатлантичного альянсу // Військово-науковий вісник. №37. 2022. С. 194-214.

12. Frost, Mervyn, Mervyn Frost, and Nicholas Michelsen // Strategic communications in international relations: practical traps and ethical puzzles // NATO Strategic Communications Centre of Excellence, 2017.

13. Північноатлантичний договір: документ від 04.04.1994 // База даних «Законодавство України» // ВР України. URL: https://zakon.rada.gov.ua/laws/show/950_008#Text. (дата звернення: 21.05.2023).

14. Sayle, Timothy Andrews // Enduring alliance: a history of NATO and the postwar global order // Cornell University Press, 2019.

15. Laity, Mark // The birth and coming of age of nato stratcom: a personal history // Defence Strategic Communications. Vol.10.10.2021. P. 21-70.

16. Kushnir, Viktoria, and Iryna Izhutova // Strategic communications: current state within security and defence sector // Reality of Politics. Vol. 16. 2021. P. 68-77.

17. Рейда, О. А. // The main elements of strategic communication system in NATO // Актуальні проблеми права в умовах сучасних викликів. 2021. С. 120.

18. Murginski, Petar // The Survival of NATO in the Post-Cold War Era: A Comparative Analysis of Neorealist and Constructivist Theories // Bulletin of national defence university. Vol. 12.1. 2023. P. 53-61.

19. NATO Strategic Concept in the Shadow of the War // Globsec. URL: https://www.globsec.org/what-we-do/publications/nato-strategic-concept-shadow-war . (дата звернення: 12.04.2023).

20. Geoana, Mircea, et al // The future of NATO after the Madrid 2022 summit // Strategy Notebook. Vol. 211. 2022. P. 45-63.

21. Risso, Linda // Squaring the Circle: The Evolution of NATO's Strategic Communication Since the 1990s // Journal Of Peace And War Studies. 2021. P. 157.

22. Hanley, Monika // NATO's Response to Information Warfare Threats. Information Wars in the Baltic States: Russia's Long Shadow // Cham: Springer International Publishing. 2022. P. 205-223.

23. Larsen, Henrik // Adapting NATO to Great-Power Competition // The Washington Quarterly 45.4. 2022. P. 7-26.

24. Doyle, Kieran, and Tedla Desta // An analysis of Common Security and Defence Policy's (CSDP) strategic communication (StratCom) // J. Pol. & L. Vol.14. 2021. P. 56.

25. Pylypchuk, V. // Theoretical and Legal Basis for the Security and Defense Strategic Communications System Development // State-Legal Sciences And International Law. Vol.12. 2020. P. 65-79.

26. Gjoreski, Igor, and Zoran Nacev // Global security trends in euro-atlantic area and nato new strategic concept // Security Dialogues. Vol. 13.2. 2022. P. 132-146.

27. Bogdanoski, M. // NATO Cyber Defence Policy and Hybrid Threats: The Way to Enhance Our Resilience // Building Cyber Resilience against Hybrid Threats. Vol. 61. 2022. P. 20-54.

28. Mitrovic, Miroslav, and Ana Vulić // Project Management of Strategic Communication in Digital Era // Project Management of Strategic Communication in Digital Era. Advances in Economics, Business and Management Research. Vol. 108. 2019. P. 76-82.

29. Unver, Akin, and Ahmet Kurnaz // Securitization of Disinformation in NATO Lexicon: A Computational Text Analysis // All Azimuth A Journal of Foreign Policy and Peace. Vol. 11. 2022. P. 211-233.

30. Maronkova, Barbora // NATO Amidst Hybrid Warfare Threats: Effective Strategic Communications as a Tool Against Disinformation and Propaganda // Disinformation and Fake News. 2021. P. 117-129.

31. Inside the Kremlin's Year of Ukraine Propaganda // Time. URL: https://time.com/6257372/russia-ukraine-war-disinformation/. (дата звернення: 28.04.2023).

32. Москві ніхто не обіцяв, що НАТО не буде розширюватися. Але їй байдуже // Радіо Свобода. URL: https://www.radiosvoboda.org/a/usa-rosija-nato-rozshyrennia/31263752.html. (дата звернення: 10.05.2023).

33. Як і навіщо російська пропаганда шукає біолабораторії США в Україні та світі? // Українська правда. URL: https://www.pravda.com.ua/columns/2022/09/22/7368473/. (дата звернення: 09.05.2023).

34. Provocation and Disinformation Overview// Vox Ukraine. URL: https://voxukraine.org/en/provocation-and-disinformation-overview. (дата звернення: 18.05.2023).

35. Vergara, Raymond John D., Philip Joseph D. Sarmiento, and James Darwin N. Lagman. // Building public trust: a response to COVID-19 vaccine hesitancy predicament // Journal of Public Health. Vol. 43.2. 2021. P. 291-292.

36. Reding, Dale F., and Bryan Wells // Cognitive warfare: NATO, COVID-19 and the impact of emerging and disruptive technologies // COVID-19 Disinformation: A Multi-National, Whole of Society Perspective. Cham: Springer International Publishingю 2022. P. 25-45.

37. Kuhn, Kristen, Salih Bicakci, and Siraj Ahmed Shaikh // COVID-19 digitization in maritime: understanding cyber risks // WMU Journal of Maritime Affairs. Vol. 20.2. 2021. P. 193-214.

38. Gottemoeller, Rose, et al // Engaging with emerged and emerging domains: cyber, space, and technology in the 2022 NATO strategic concept // Defence Studies. Vol. 22.3. 2022. P. 516-524.

39. Russia’s Cyber Tactics: Lessons Learned 2022 // Аналітичний звіт Держспецзв'язку про рік повномасштабної кібервійни росії проти України. State Service of Special Communications and Information Protection of Ukraine. 2023. 33 p.

40. World's largest cyber defense exercise Locked Shields brings together over 3000 participants // CCDCOE. URL: https://ccdcoe.org/news/2023/6016/. (дата звернення: 12.05.2023).

41. Варшавська декларація НАТО // Європейська правда. URL: https://www.eurointegration.com.ua/articles/2016/07/9/7051894/. (дата звернення: 24.03.2023).

42. НАТО на кіберзахисті: як Альянс допомагає Україні вберегтися від хакерських атак РФ // Європейська правда. URL: https://www.eurointegration.com.ua/articles/2022/07/6/7142651/. (дата звернення: 02.05.2023).

43. Alexandra-Cristina, D. I. N. U. // Cyber Diplomacy and Artificial Intelligence: Opportunities and Challenges // International Conference on Cybersecurity and Cybercrime. Vol. 10. 2023.

44. Jacobsen, Jeppe T. // Cyber offense in NATO: challenges and opportunities // International affairs. Vol. 97.3. 2021. P. 703-720.

45. Guenther, Lindsey, and Paul Musgrave // New Questions for an Old Alliance: NATO in Cyberspace and American Public Opinion // Journal of Global Security Studies. Vol. 7.4. 2022. P. 24-35.

46. Офіційний сайт НАТО. URL: https://www.nato.int/cps/en/natohq/index.htm. (дата звернення: 21.04.2023).

47. Країни НАТО створюють інноваційний фонд: для початку готові вкласти у проєкти 1 млрд дол США // Dsnews.ua. URL: https://www.dsnews.ua/ukr/world/strany-nato-sozdayut-innovacionnyy-fond-dlya-nachala-gotovy-vlozhit-v-proekty-1-mlrd-30062022-461884 (дата звернення: 04.05.2023).

48. Нова Стратегічна концепція Альянсу: у пріоритеті агресія рф в Україні // Армія Inform. URL. https://armyinform.com.ua/2022/07/09/nova-strategichna-konczepcziya-alyansu-u-prioryteti-agresiya-rf-v-ukrayini/. (дата звернення: 19.05.2023).

49. Filho, Walter Leal, et al // Deploying digitalisation and artificial intelligence in sustainable development research // Environ. Dev. Sustain. 2022. Vol. 25(6). P. 457-488.

50. Christie, Edward, and Amy Ertan // NATO and Artificial Intelligence // Routledge Companion to Artificial Intelligence and National Security Policy. Routledge. Forthcoming. 2021. 19 p.

51. Alexiyevets, Lesya, and Mykola Alexiyevets // Ukraine–the NATO: mutual relations and partnerships main stages // East European Historical Bulletin. Vol. 14. 2020. P. 175-189.

52. Про внесення змін до Конституції України (щодо стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору): закон України // Відомості Верховної Ради (ВВР), 2019, № 9, ст.50. URL: https://zakon.rada.gov.ua/rada/show/2680-19#Text. (дата звернення: 03.04.2023).

53. Lepskiy, Maxim, and Nataliia Lepska // The War in Ukraine and its Challenge to NATO: Peacekeeping to Peace Engineering // American Behavioral Scientist. Vol. 67.3. 2023. P. 402-425.

54. Khorishko, Liliia Serhiivna // Strategic Communications Of Ukraine In The Cotext Of The Russian-Ukrainian War // Publishing House «Baltija Publishing». 2022.

55. Lomidze, Mariam // Georgia's and Ukraine's EU and NATO Integration Perspectives // Травневі студії: історія, політологія, міжнародні відносини. 2022. P. 85-86.