УДК 327
DOI https://doi.org/10.20535/2308-5053.2023.2(58).285605

СПІВРОБІТНИЦТВО УКРАЇНИ ТА НАТО У ПРОТИДІЇ ДЕСТРУКТИВНИМ ІНФОРМАЦІЙНИМ ВПЛИВАМ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ (2022–2023 РР.)

Максимець В. Є.,
кандидат політичних наук, доцент,
доцент кафедри міжнародної інформації
Національного університету «Львівська політехніка»
ORCID ID: 0000-0002-9003-7055
vira.y.maksymets@lpnu.ua

Вівсяна В. І.,
студентка кафедри міжнародної інформації
Національного університету «Львівська політехніка»
ORCID ID: 0009-0000-6881-0390
viktoriia.vivsiana.mnmim.2021@lpnu.ua

Дослідження присвячено аналізу досвіду НАТО щодо протидії інформаційним загрозам, оскільки сучасний рівень розвитку вимагає колективної боротьби з поширенням інформації, використанням її як одного з видів ведення війни. З розвитком технологій і еволюцією каналів зв'язку розповсюдження інформації стає дедалі складнішим. Показано, що НАТО визнала необхідність адаптувати свої стратегії та можливості для ефективного протистояння викликам, пов'язаним з дезінформацією, пропагандою та кібероперація̈ми та розширити свій інструментарій з протидії гібридним загрозам.

У статті проаналізовано потенціал партнерства Україна-НАТО у боротьбі з російською пропагандою, їх співробітництво у сфері інформаційної безпеки: спільні інтереси, тенденції. Також охарактеризовано основні виклики та загрози співпраці між Україною та НАТО та визначено рамки співпраці між Україною та НАТО у сфері кіберзахисту. Потік російської дезінформації значно зріс після початку повномасштабної війни росії в Україні. Проте Україна почала зміцнювати своє інформаційне та медіа-середовища ще з 2014 року, і почала працювати над механізмами для боротьби з інформаційними загрозами. Дезінформаційні кампанії росії спрямовані на те, щоб спричинити розколи всередині України та між іншими урядами. Важливо зазначити, що Північноатлантичний Альянс також зазнає російської пропаганди. Для прикладу, російські ЗМІ поширюють наступну інформацію: 1) мета Майдану - створення баз НАТО в Криму; 2) НАТО розмістило в Україні лабораторію біологічної зброї; 3) спецслужби НАТО працювали над викраденням Україною російських літаків; 4) НАТО вважає Україну одноразовим інструментом для війни з росією та інші. Тобто слід зауважити, що інформація та її поширення відіграє важливу роль для держав та міжнародних організацій для поширення власних інтересів та досягнення цілей.

Автори подають основні рекомендації щодо посилення протистояння дезінформації, що може використовувати будь-який актор міжнародних відносин. У результаті обгрунтовано, що держави мають працювати над створенням нової установи, яка би була автономною та могла б проводити аналіз даних, необхідний для забезпечення незалежного контролю, якого вимагають нові політичні рамки; потрібно розвивати медіаграмотність населення; необхідно, щоб технологічні компанії такі як Meta, YouTube та Twitter, дотримувалися своєї політики щодо заборони дезінформації фінансованої рекламою.

Ключові слова: НАТО, інформаційні загрози, кіберзахист, росія, пропаганда, оборона, стримування, інформаційна безпека.

Постановка проблеми. Враховуючи сучасний стан міжнародних відносин та швидке поширення використання мережі інтернет дедалі частіше піднімається питання інформаційної безпеки, як на національному так і на міжнародному рівнях. Для кожного суб'єкта міжнародних відносин важливо

створити захищений інформаційний простір, а також мати можливість протидіяти інформаційним загрозам, які можуть завдати шкоди, як окремому суб'єкту так і державі загалом. Через швидкий розвиток сучасних технологій стає все складніше протидіяти інформаційним загрозам власноруч. Тому досить важливо кооперувати зусилля на міжнародному рівні аби завжди бути готовим до протидії новим загрозам.

Насправді, інформація є потужним інструментом, який порушує національний інформаційний суверенітет. НАТО – організація, яка створена для забезпечення безпеки держав-членів та союзників. Саме тому члени Альянсу продовжують створювати нові інструменти для боротьби з інформаційними загрозами. Протягом багатьох років НАТО розробила багатогранний підхід, який охоплює розробку політики, посилення співпраці та оперативні можливості. Ключові елементи підходу НАТО включають формування стійкості в державах-членах шляхом підвищення їхньої медіаграмотності, сприяння критичному мисленню та сприяння журналістиці, заснованій на фактах. НАТО також розширила співпрацю зі стратегічними партнерами, міжнародними організаціями та громадянським суспільством для обміну передовим досвідом, інформацією та координації реагування на інформаційні загрози. Для прикладу, НАТО стали використовувати соціальні мережі для боротьби з дезінфомацією, створювати нові органи, такі як Центр передового досвіду в галузі стратегічних комунікацій НАТО (NATO StratCom Centre of Excellence), ухвалювати нові стратегії та співпрацювати з міжнародними партнерами для взаємного обміну інформацією та обміну досвідом.

НАТО та його союзники покладаються на сильний та стійкий кіберзахист для виконання основних завдань Альянсу щодо колективної оборони, управління кризою та спільної безпеки. НАТО має бути готовим захищати свої мережі та операції від зростаючої кількості кіберзагроз, з якими він стикається. В основному НАТО приділяє увагу захисту власних мереж, а також роботі в кіберпросторі (у тому числі в рамках операцій і місій), допомозі союзникам підвищити свою національну стійкість і забезпечити платформу для політичних консультацій і колективних дій. Ну і загалом складність та гібридний характер інформаційних загроз спонукає міжнародні організації змінювати підхід до політики у сфері інформаційної безпеки, до того ж необхідно формувати нові структури аби мати можливість швидко та безперешкодно протидіяти сучасним викликам, які можуть порушити мир та стабільність у світі.

Аналіз останніх досліджень і публікацій. У вітчизняній і зарубіжній дослідницькій літературі існує багато робіт, які присвячені різним аспектам співробітництва України та НАТО. Серед досліджень українських науковців слід зазначити праці: О. Білоруса, В. Горбуліна, Г. Перепелиці, В. Раденького, А. Риженка, О.Соскіна, А. Шевцова, та інших. Разом із зростанням інформаційних загроз, зростає і база досліджень, яка стосується даного питання. Серед таких досліджень виділяємо роботи Н. Бєлоусова, П. Афанасьєва, М. Ожеван, а також М. Гуцалюк, М. Кравцов та інші.

Мета статті – проаналізувати виклики та загрози співпраці між Україною та НАТО та розглянути досвід НАТО щодо протидії інформаційним загрозам з метою надання рекомендацій у протидії деструктивним інформаційним впливам російської федерації.

Виклад основного матеріалу. На сучасному етапі безпека інформаційного простору є ключовим завданням, оскільки вона стосується як пересічного громадянина, так і конкретної держави, або групи держав. Все частіше питання інформаційних загроз піднімають на міжнародних конференціях, самітах та на рівні міжнародних організацій. Тому що, шкідлива кіберактивність поширюється досить швидко, починаючи від програм, які допомагають злодіям здобути приватну інформацію, до шпигунства та кібератак, які мають політичну мету.

НАТО – військово-політична організація, яка створена підтримувати міжнародний мир та безпеку. Саме тому Альянс працює в одну ногу з сучасними загрозами безпеці, а успішна діяльність НАТО неможлива без правдивої інформація. Навіть миротворчі операції НАТО є більш успішними через обізнаність громадян у цьому питанні і в результаті це сприяє більшій ефективності.

Існує безліч загроз, які спонукають Альянс вживати нових заходів у боротьбі з кіберзагрозами. Однією з таких загроз в інформаційній безпеці демократичним державам можна згадати росію. Наприклад, якщо брати до уваги політично мотивовані кібератаки, то одним з прикладів є зламана електронна пошта норвезького парламенту у 2020 році. Цей інцидент був названий як такий, що вплинув на найважливіший демократичний інститут країни. Пізніше норвезька влада визначила росію як державу, яка винна за напад.

З початку 2022 року український уряд зазнав серії кібератак, які призвели до зіпсування урядових веб-сайтів та знищення даних на деяких державних комп'ютерах. У середині січня хакери зламали близько 70 українських веб-сайтів, у тому числі міністерств закордонних справ, оборони, енергетики, освіти та науки, а також ДСНС та Міністерства цифрової трансформації, портал електронного урядування якого надає український публічний цифровий доступ до десятків державних послуг. Міжнародний колектив хактивістів Anonymous оголосив «кібервійну» проти російського уряду,

визнаючи заслугу за кілька кіберінцидентів, включаючи поширені атаки відмови в обслуговуванні, які знищили російські урядові веб-сайти та державну службу новин Russia Today.

Кібератаки на Естонію в 2007 році вивели з ладу її урядові, медіа та фінансові веб-сайти, далі росія анексувала чистину території Грузії у 2008 році і був проведений ряд кібератак на грузинські веб-сторінки. Саме тоді члени Альянсу почали розуміти, що вони не готові до такого роду викликів.

Тому починаючи з 2007 року НАТО вирішило стати більш активним користувачем соціальних мереж таких як Facebook, YouTube та Twitter. До того ж було вирішено створити телеканал та сайт куди завантажували розсекречені відеозаписи операцій. Така діяльність давала змогу протидіяти дезінформації, яку поширювали країни-противники Альянсу.

У січні 2008 року НАТО затвердила свою першу політику щодо кіберзахисту. Члени НАТО підкреслили, що настав етап, коли надзвичайно важливо аби інформаційні системи були в безпеці Тому необхідно ділитися передовим досвідом, і допомагати державам-союзникам у боротьбі з кібератакам.

Російська агресія проти України починаючи з окупації Криму, а зараз вже і повномасштабна війна ввесь час супроводжується інформаційними операціями на всіх етапах. Саме тому ще у 2014 НАТО почало свою діяльність зі створення Центру передового досвіду в галузі стратегічних комунікацій НАТО у Ризі (StratCom Centre of Excellence). Діяльність даної структури спрямована на пошук шляхів розв'язання проблем, важливо, що вони приділяють увагу російській агресії проти України (About NATO StratCom COE, 2022). StratCom сприяє покращенню можливостей стратегічного зв'язку в Альянсі та країнах-членах. Стратегічне спілкування є невід'ємною частиною зусиль, спрямованих на досягнення політичних і військових цілей Альянсу, тому стає все більш важливим, щоб Альянс належним, своєчасним, точним і відповідальним чином повідомляв про свої цілі та місії. Основними напрямками діяльності за 2021 рік є: 1) експеримент багатонаціональних інформаційних операцій; 2) розробка концепції моделювання інформаційного середовища; 3) розробка концепції навчального модуля моделювання дезінформаційної атаки; 4) курс та конференція в соціальних мережах (About NATO StratCom COE, 2022).

Також діяльність НАТО StratCom Centre of Excellence спрямована не лише на захист держав-членів, але й на партнерів, оскільки цей орган можна вважати таким, що надає підтримку державам-членам, кожна з яких має можливість розбудовувати власну систему інформаційного захисту.

У 2015 році було ухвалено стратегію щодо протидії гібридній війні і після цього країни-члени розпочали розширювати набір інструментів НАТО для реагування на ці загрози, які включають в себе дезінформацію та кібератаки.

Пізніше у 2016 році на саміті НАТО члени підтвердили оборонний мандат НАТО і визнали кіберпростір як область операцій, у якій НАТО має захищати себе так само ефективно, як в повітрі, на землі або воді. Оскільки більшість криз і конфліктів сьогодні мають кібервимір (Zhadan, 2022).

На саміті НАТО 2021 року було схвалено нову Всеосяжну політику кіберзахисту, яка підтримує три основні завдання НАТО: колективну оборону, врегулювання криз і спільну безпеку, а також її загальну позицію стримування та оборони. Оборонний мандат НАТО було підтверджено, і члени Альянсу взяли на себе зобов'язання використовувати весь спектр можливостей для активного стримування, захисту та протидії всьому спектру кіберзагроз у будь-який час. Цікавим є те, що члени НАТО розглядають злочинний вплив кіберактивності, як збройний напад (About NATO StratCom COE, 2022).

Важливо зазначити, що і НАТО і Україна досить часто підпадають під Кремлівську пропаганду з метою дезінформації суспільства, і вкорінення в суспільство думок, що Альянс є ворожою небезпечною організацією, а Україна це тимчасова зброя НАТО за допомогою якої Альянс веде боротьбу проти рф.

Наприклад, росія стверджувала, що розпочала СВО, щоб запобігти розміщенню військових баз НАТО в Україні. Але зараз російські медіа та експерти намагаються переконати своїх громадян, що головна мета війни - запобігти знищенню Росії НАТО. У такий спосіб, Україна стає суб'єктом пропаганди росії. Ця дезінформація поширюється, щоб утворити враження, що СВО є «священною народною війною» і спонукати росіян до військових дій, а НАТО – загроза для всієї росії (Фейки, 2023).

Ще одна тенденція російської дезінформації – це ствердження, що Збройні сили України ведуть боротьбу виключно в інтересах НАТО. Раніше російські ЗМІ твердили, що росія воює проти НАТО, що Альянс керує Збройними силами України, а в їх складі беруть участь найманці з інших країн. Нова теза полягає в тому, що росія воює саме проти України, але українці захищають не свої інтереси, а інтереси США та інших країн НАТО. Пропагандисти намагаються наголосити на визначальній ролі НАТО в цьому конфлікті, хоча вони визнають суб'єктність України та Збройних сил (Фейки, 2023). До того ж, російської дезінформації має на меті змінити сприйняття українцями причин війни на Донбасі та анексії Криму. Російські пропагандисти намагаються перекласти відповідальність за конфлікт на НАТО та викликати недовіру до західних держав. Це може спричинити подальше роз'єднання між Україною та західним світом, що сприятиме інтересам росії.

Важливо розуміти, що ці тези є неправдивими та є частиною гібридної війни, яку росія веде проти України та Альянсу. Ці зусилля з метою дезінформації та впливу на суспільні думки мають негативний вплив на ситуацію в регіоні та загострюють конфлікт. Саму тому надзвичайно важливо розуміти правдиву природу війни та її причин, щоб знайти шляхи до миру та стабільності.

Загалом співпраця між Україною та НАТО стикається зі значними викликами та загрозами, але обидві сторони залишаються відданими працювати разом, щоб подолати ці виклики та посилити безпеку в регіоні.

Варто згадати, ще один приклад, як фахівці НАТО реагують на інформаційні операції ворога, та спростовують фейкову інформацію шляхом поширення правдивих повідомлень різними каналами, аби досягнути різних цільових аудиторій. Важливим також є те, що Альянс намагається створити «інформаційнй імунітету», який зробить населення більш стійким до ворожих повідомлень, за допомогою яких ворог намагається переконати суспільство у негативному ставленні до НАТО. Одним з прикладів слід згадати дезінформацію з приводу COVID-19, яку поширювали Росія та Китай. Про те, що вірус виник або в Європі, або в США. Цікавим прикладом є те, що у період COVID-19 НАТО було скоординовано кілька інформаційних атак. По-перше, атака була проти присутності військ НАТО в Польщі Латвії та Литві. Саме тоді до міністра оборони Литви було направлено листа нібито від генерального секретаря НАТО в якому зазначалося про плани НАТО вивести війська з країни. По-друге, було створене неправдиве інтерв'ю, що нібито канадські війська занесли вірус до в Латвії. І по-третє, був відправлений лист де нібито польський військовий критикує американські війська (Cyber, 2022).

У боротьбі з такими видами дезінформації НАТО має сайт під назвою «Setting the Record Straight». На цьому інтернет ресурсі можна знайти усі виступи, інтерв'ю, відео та зображення, які спростовують усю дезінформацію. Важливо, що на цьому сайті інформація публікується кількома мовами, щоб кожен міг знайти правдиву інформацію. До того ж НАТО завжди просить ЗМІ виправити неправдиві історії. Звичайно такі методи не допоможуть зупинити потік фейкової інформації, але важливо викрити неправдиву та презентувати правдиву інформацію підтверджену фактами.

Слід звернути увагу на наступні кроки НАТО у боротьбі з інформаційними загрозами. По-перше, НАТО має службу реагування на кіберінциденти, яка базується у Бельгії. Дана служба захищає особисті мережі НАТО, і також надає централізовану та цілодобову підтримку.

По-друге, НАТО також створило Центр операцій у кіберпросторі. Цей центр підтримує зв'язок з військовими командирами, які мають інформацію стосовно операцій та місій і тому можуть передавати інформацію Альянсу, а також центр забезпечує свободу дій у кіберсфері та робить операції більш стійкими до кіберзагроз (NATO's, 2020).

Досить важливо, що НАТО співпрацює з різними міжнародними акторами, а саме з міжнародними організаціями такими як ЄС або ж з країнами-партнерами, такими як Україна, Фінляндія або ж Швеція задля більш ефективного результату у боротьбі з кіберзагрозами. НАТО також присутнє у кооперації з партнерами в Азіатсько-Тихоокеанському регіоні для обміну досвідом щодо національних підходів до протидії гібридним загрозам, таким як збільшення кількості дезінформації та кібератак. Це було особливо цінно в контексті пандемії COVID-19.

Наприклад між НАТО та ЄС у 2016 році була укладена Технічна угода з кіберзахисту між NATO Computer Incident Response Capability (NCIRC) та Computer Emergency Response Team of the European Union (CERT-EU). Метою даної угоди є посилення кіберзахисту обох організацій шляхом обміну даними, що стосуються обговорюваної сфери. Важливо, що дана угода передбачає не тільки обмін інформацією про конкретні кіберзагрози, а також і передовий досвід щодо технічних процедур. До того ж співпраця НАТО та ЄС також розширюється у сфері навчання та досліджень, які мають відчутні результати у протидії кіберзагрозам (Pernik, 2014).

Важливо зазначити, що у Фінляндії розташований Європейський центр протидії гібридним загрозам, який було створено у 2017 році представниками країн НАТО та ЄС. Даний центр займається проведенням досліджень, аналізом гібридних загроз та визначенням методів боротьби з ними. Наступною діяльністю центру є проведення консультацій на стратегічному рівні між учасниками ЄС та НАТО (Паршикова, 2018).

Загалом НАТО та ЄС мають будувати ефективний діалог необхідний для взаємного обміну інформацією, звітування про різні інциденти, управління надзвичайними ситуаціями та кризовими ситуаціями, а також для проведення спільних тренінгів і навчань.

У 2022 року Агентство зв'язку та інформації НАТО та Україна підписали Меморандум про угоду, який зосереджується на співпраці в проектах, пов'язаних з технологіями. Ця угода спрямована на зміцнення партнерства між НАТО та Україною шляхом надання допомоги в модернізації її інформаційних технологій та послуг зв'язку. Крім того, меморандум містить положення щодо визначення областей, де може знадобитися навчання особового складу, а також навчання, семінари та тематична експертиза для підтримки зусиль України щодо модернізації її обороноздатності (Кудіна, 2022).

Крім того, у 2022 році НАТО оприлюднила нову програму швидкого реагування на кібератаки, в рамках якої пообіцяла посилити кіберзахист України перед обличчям російських кібератак, які тривають. Оновлено Комплексний пакет допомоги НАТО Україні, ключовим компонентом є Трастовий фонд кібербезпеки. НАТО зосередиться на розвитку можливостей України, забезпеченні необхідним обладнанням і навчанні персоналу у сфері кібербезпеки. Ця підтримка спрямована на те, щоб допомогти Україні захистити свою інфраструктуру від сучасних кіберзагроз.

До того ж, Угода про Трастовий фонд кіберзахисту є досить важливим механізмом співпраці Україна-НАТО у сфері кіберзахисту. Угода передбачає фінансову підтримку проектів, спрямованих на покращення можливостей кіберзахисту, таких як створення навчального центру з кібербезпеки та розробка національної стратегії кібербезпеки (У НАТО, 2017).

Хоча кібератаки росії проти України не були такими значними, як її звичайні військові дії, НАТО не може дозволити собі нехтувати потужним кіберзахистом. Атака Голового управління Генерального штабу ЗС рф NotPetya у 2017 році була спрямована на Україну, але зрештою завдала глобальної шкоди західним компаніям у сумі збитків приблизно в 10 мільярдів доларів. Використання проксі-серверів для наступальних кібероперацій Росією демонструє постійну небезпеку в кіберсфері. Якщо російські військові продовжуватимуть боротися проти України, а санкції Заходу продовжуватимуть впливати на російську економіку, існує ймовірність того, що путін може посилити наступальні кібератаки з боку кібератак проти НАТО та Заходу. Такі атаки на критичну інфраструктуру та промислові системи контролю можуть мати руйнівні наслідки як для НАТО так і для України (Banks, 2022).

Важливо враховувати, що серія кібератак між росією і НАТО може призвести до циклу ескалації, в результаті якого росія може застосувати хімічну зброю або навіть тактичну чи ядерну зброю малої потужності. Росія попередила адміністрацію США про припинення надання сучасної зброї українським військам ще 15 квітня 2022 року і пригрозила «непередбачуваними наслідками». Це свідчить про те, що росія може спробувати націлити або саботувати деякі з цих поставок зброї, перебуваючи на території НАТО, або атакувати НАТО в інший спосіб, можливо, за допомогою кіберзасобів. Такий напад також можна вважати збройним (Klipstein, 2022).

Враховуючи вище зазначене, слід додати, що зацікавленим акторам варто звернути увагу на наступні рекомендації стосовно боротьби з дезінформацією:

1) держави мають працювати над створенням нової установи, яка би була автономною та могла б проводити аналіз даних, необхідний для забезпечення незалежного контролю, якого вимагають нові політичні рамки;

2) потрібно розвивати медіаграмотність населення для того щоб громадяни розуміли, як орієнтуватися в інформаційному середовищі та мати доступ до достовірної, перевіреної інформації;

3) необхідно створити сильні системи моніторингу, які могли б отримувати потоки дезінформації в усьому інформаційному середовищі кількома мовами;

4) необхідно, щоб технологічні компанії такі як Meta, YouTube та Twitter, дотримувалися своєї політики щодо заборони дезінформації фінансованої рекламою;

5) фінансування незалежної журналістики та перевірки фактів - ще один важливий крок у боротьбі з дезінформацією.

Висновки. Загалом, досвід НАТО у протидії деструктивним інформаційним загрозам підкреслює важливість раннього виявлення і швидких і рішучих дій. Альянс визнає, що кампанії з дезінформації та інші інформаційні загрози можуть мати значний вплив на країни-члени і їх населення, і вживає заходів з посилення своєї стійкості і готовності до протидії таким загрозам. Зусилля НАТО демонструють відданість організації протидії інформаційним загрозам і захисту безпеки її членів.

Взаємини між Україною та НАТО мають багатогранну історію, яка відображає сучасні виклики та потреби міжнародної системи безпеки та розвитку. Ці відносини пройшли довгий шлях, розпочавши з програми «Партнерство заради миру», і досягли важливої точки з підписанням Хартії про особливе партнерство між Україною та НАТО. Нині ця взаємодія є ширшою і включає співпрацю у різних сферах, включаючи політичну, військову, військово-технічну та інші. Зокрема, в контексті збройної агресії росії проти України, співпраця з НАТО має важливе значення для підтримки безпекових спроможностей України.

Maksymets V., Vivsiana V. Cooperation between Ukraine and NATO in countering destructive iInformational influences of the Russian Federation (2022–2023)

The research analyses NATO's experience in countering information threats, since the current level of development requires a collective fight against the spread of information, using it as a form of warfare. The spread of information is becoming increasingly complex due to the development of technology and the

evolution of communication channels. It is show that NATO has recognized the need to adapt its strategies and capabilities to effectively counter the challenges posed by disinformation, propaganda and cyber operations and to expand its tools to counter hybrid threats.

The article analyses the potential of the NATO-Ukraine partnership in the fight against Russian propaganda, their cooperation in the field of information security: common interests and trends. It also describes the main challenges and threats to NATO-Ukraine cooperation and defines the framework for NATO-Ukraine cooperation in cyber defense. The flow of Russian disinformation has increased significantly since the start of Russia's full-scale war in Ukraine. However, Ukraine began strengthening its information and media environment as early as 2014, and began working on mechanisms to combat information threats. Russia's disinformation campaigns are aimed at causing divisions within Ukraine and between other governments. It is important to note that the North Atlantic Alliance is also subject to Russian propaganda. For example, the Russian mass media spread the following information: 1) the purpose of the Maidan is to create NATO bases in Crimea; 2) NATO placed a biological weapons laboratory in Ukraine; 3) NATO special services worked on the hijacking of Russian planes by Ukraine; 4) NATO considers Ukraine a disposable tool for war with Russia and others. That is, it should be noted that information and its dissemination play an important role for states and international organizations to spread their own interests and achieve goals.

The authors provide key recommendations for strengthening the counteraction to disinformation that can be used by any actor in international relations. As a result, it is argued that states should work to create a new autonomous institution that can conduct the data analysis necessary to ensure the independent control required by the new policy framework; media literacy should be developed; and technology companies such as Meta, YouTube and Twitter should adhere to their policies on prohibiting disinformation funded by advertising.

Key words: NATO, information threats, cyber defense, Russian propaganda, deterrence, information security, countering.

Література:

1. About NATO StratCom COE. *NATO Strategic Communications Centre of Excellence: web-site.* URL: https://stratcomcoe.org/about_us/about-nato-stratcom-coe/5
2. Zhadan A. Countries brace for cyberattacks as Sweden and Finland move to join NATO. *Latest Cybersecurity and Tech News, Research & Analysis.* 2022. May 17. URL: https://cybernews.com/cyber-war/countries-brace-for-cyberattacks-as-sweden-and-finland-move-to-join-nato/
3. Фейки про НАТО та Україну: як змінила акценти російська пропаганда у Криму. *Укрінформ.* 2023. April 10. URL: https://www.ukrinform.ua/rubric-crimea/3693944-fejki-pro-nato-ta-ukrainu-ak-zminila-akcenti-rosijska-propaganda-u-krimu.html
4. Cyber defence. *North Atlantic Treaty Organization: web-site.* 2022. March 23. URL: https://www.nato.int/cps/en/natohq/177273.htm
5. NATO's response to hybrid threats. *North Atlantic Treaty Organization: web-site*. 2020. March 16. URL: https://www.nato.int/cps/en/natohq/topics_156338.htm
6. Pernik P. Improving Cyber Security: NATO and the EU. *International Centre for Defence Studies.* 2014. URL: https://icds.ee/wp-content/uploads/2010/02/Piret_Pernik_-_Improving_Cyber_Security.pdf
7. Паршикова. А. Міжнародний досвід протидії гібридним загрозам: законодавче регулювання та організації з питань стратегічних комунікацій. Інформаційно-дослідницький центр. URL: https://infocenter.rada.gov.ua/uploads/documents/29377.pdf
8. Кудіна М. НАТО посилюватиме кіберзахист України у гібридній війні з РФ. *Інтернет Свобода.* 2022. July 07. URL: https://netfreedom.org.ua/article/nato-posilyuvatime-kiberzahist-ukrayini-u-gibridnij-vijni-z-rf
9. У НАТО створено фонд допомоги Україні в сфері кібербезпеки. *Голос Америки.* 2017. June 28. URL: https://ukrainian.voanews.com/a/nato-ukrayina-kiberbezpeka/3919542.html
10. Banks W. Cyberattacks and the Russian War in Ukraine: The Role of NATO and Risks of Escalation. *Georgetown Journal of International Affairs.* 2022. August 08. URL: https://gjia.georgetown.edu/2022/08/08/cyberattacks-and-the-russian-war-in-ukraine-the-role-of-nato-and-risks-of-escalation%EF%BF%BC/
11. Klipstein M., Japaridze T. Collective cyber defence and attack: NATO's Article 5 after the Ukraine conflict. *European Leadership Network.* 2022. May 16. URL: https://www.europeanleadershipnetwork.org/commentary/collective-cyber-defence-and-attack-natos-article-5-after-the-ukraine-conflict/

References:
1. About NATO StratCom COE. Official site of NATO Strategic Communications Centre of Excellence. URL: https://stratcomcoe.org/about_us/about-nato-stratcom-coe/5
2. Zhadan A. (2022, May 17). Countries brace for cyberattacks as Sweden and Finland move to join NATO. Latest Cybersecurity and Tech News, Research & Analysis. URL: https://cybernews.com/cyber-war/countries-brace-for-cyberattacks-as-sweden-and-finland-move-to-join-nato/
3. Feiky pro NATO ta Ukrainu: yak zminyla aktsenty rosiiska propahanda u Krymu. (2023, April 10). [Fakes About NATO and Ukraine: how Russian Propaganda Changed the Emphasis in Crimea]. *Ukrinform.* URL: https://www.ukrinform.ua/rubric-crimea/3693944-fejki-pro-nato-ta-ukrainu-ak-zminila-akcenti-rosijska-propaganda-u-krimu.html [in Ukrainian].
4. Cyber defence. (2022, March 23). Official site of North Atlantic Treaty Organization. URL: https://www.nato.int/cps/en/natohq/177273.htm
5. NATOs response to hybrid threats. (2020, March 16). Official site of North Atlantic Treaty Organization. URL: https://www.nato.int/cps/en/natohq/topics_156338.htm
6. Pernik P. (2014). Improving Cyber Security: NATO and the EU. *International Centre for Defence Studies.* URL: https://icds.ee/wp-content/uploads/2010/02/Piret_Pernik_-_Improving_Cyber_Security.pdf
7. Parshykova. A. Mizhnarodnyi dosvid protydii hibrydnym zahrozam: zakonodavche rehuliuvannia ta orhanizatsii z pytan stratehichnykh komunikatsii. [International Experience of Countering Hybrid Threats: Legislative Regulation and Organizations on Issues of Strategic Communications]. Informatsiino-doslidnytskyi tsentr. URL: https://infocenter.rada.gov.ua/uploads/documents/29377.pdf [in Ukrainian].
8. Kudina M. (2022, July 07). NATO posyliuvatyme kiberzakhyst Ukrainy u hibrydnii viini z RF. [NATO will Strengthen Ukraine's Cyber Defense in a Hybrid War with the Russian Federation.] *Internet Svoboda.* URL: https://netfreedom.org.ua/article/nato-posilyuvatime-kiberzahist-ukrayini-u-gibridnij-vijni-z-rf [in Ukrainian].
9. U NATO stvoreno fond dopomohy Ukraini v sferi kiberbezpeky. (2017, June 28). [NATO has created a fund to help Ukraine in the field of cyber security]. Holos Ameryky. URL: https://ukrainian.voanews.com/a/nato-ukrayina-kiberbezpeka/3919542.html [in Ukrainian].
10. Banks W. (2022, August 08). Cyberattacks and the Russian War in Ukraine: The Role of NATO and Risks of Escalation. Georgetown Journal of International Affairs. URL: https://gjia.georgetown.edu/2022/08/08/cyberattacks-and-the-russian-war-in-ukraine-the-role-of-nato-and-risks-of-escalation%EF%BF%BC/
11. Klipstein M., Japaridze T. (2022, May 16). Collective cyber defence and attack: NATOs Article 5 after the Ukraine conflict. European Leadership Network. URL: https://www.europeanleadershipnetwork.org/commentary/collective-cyber-defence-and-attack-natos-article-5-after-the-ukraine-conflict/

Стаття надійшла до редакції 26.05.2023
Стаття рекомендована до друку 08.06.2023