DOI: https://doi.org/10.26565/1992-2337-2023-2-07
УДК 351

Грановський Микола Володимирович,
аспірант кафедри політології та філософії
навчально-наукового інституту "Інститут державного управління"
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна
e-mail: granowski_m@ukr.net https://orcid.org/0000-0002-8554-7456

СУЧАСНІ МЕХАНІЗМИ, ЯКІ ВИКОРИСТОВУЄ ЄВРОПЕЙСЬКИЙ СОЮЗ ДЛЯ БОРОТЬБИ З ГІБРИДНИМИ ЗАГРОЗАМИ

Анотація. У сучасному світі спостерігається тенденція до значного зростання кількості гібридних конфліктів, які стають все більш витонченими й непередбачуваними.

Ця стаття присвячена аналізу практичних механізмів протидії гібридним загрозам, у тому числі з боку державних органів, зокрема, у країнах ЄС.

Сучасна практика гібридних операцій з боку агресора демонструє кардинальну зміну тактики та засобів, які використовує держава-гравець світового рівня проти супротивника, який є слабким і нездатним захищати цілісність власної території.

Ключові слова: безпека; гібридна війна; гібридний конфлікт; гібридні дії; гібридні операції; тероризм.

Постановка проблеми. Початок XXI ст. характеризується новими викликами у сфері міжнародної безпеки. Вважається, що припинення «холодної війни» не ліквідувало внутрішніх або регіональних джерел конфліктів і не забезпечило стабільного мирного співіснування країн у світі. На думку експертів, міжнародне співтовариство стикається не стільки з прямим збройним конфліктом, скільки з одним із різновидів військових операцій, які можна також назвати гібридними.

Аналіз останніх досліджень і публікацій. Дослідженню трансформацій форм та характеру війн і воєнно-політичних конфліктів нового покоління («гібридних війн») присвячено доробки зарубіжних учених Я. Берзніса, Р. Глена, Ф. Гоффмана, Дж. Калха, Ф. Ван Каппена, М. Кревельда, Т. Мак Куєна, У. Лінда, Дж. Метіса, У. Немета, Е. Тоффлера, Т. Хубера та ін.

Як цитувати: Грановський М. В. Сучасні механізми, які використовує Європейський Союз для боротьби з гібридними загрозами. *Державне будівництво.* 2023. № 2 (34). С. 80–94. DOI: https://doi.org/10.26565/1992-2337-2023-2-07

In cites: Hranovskyi, M.V. (2023). Modern mechanisms used by the EU to combat hybrid threats. *State Formation, no. 2 (34), 80–94.* DOI: https://doi.org/10.26565/1992-2337-2023-2-07 [in Ukrainian].

Широке застосування способів та методів воєнно-політичних конфліктів гібридного типу для вирішення міждержавних проблем на сучасному етапі спонукали також вітчизняних науковців до поглибленого їхнього аналізу. Так, дослідженню питань «гібридної війни» присвячені роботи В. Горбуліна, Ю. Климчука, Г. Луцишини, Є. Магди, Б. Парахонського, Г. Перепелиці, Г. Ситника, А. Слюсаренка, Л. Смоли, М.Требіна, Г. Яворської та ін.

Метою статті є проведення аналізу гібридних агресій та досвіду іноземних держав щодо протидії їм, у тому числі через прийняття відповідних рішень державними органами, спрямованих на протидію невизначеному, і тим самим підступним, ворогом, який вказує, що об'єкти гібридних операцій не мали можливості використовувати стандартні тактики, а парадигму безпеки, яка була заснована на традиційних військових технологіях державних систем оборони та методах ведення військових операцій, було повністю підірвано.

Виклад основного матеріалу. З 2016 року Європейський Союз мобілізує свої ресурси та створює нові інструменти для боротьби з гібридними загрозами. Ці дії є, перш за все, реакцією ЄС на дестабілізуючі кроки Росії, Китаю та менших країн, зокрема: Білорусі, Ірану та Північної Кореї.

Діяльність Європейського Союзу досі була зосереджена на боротьбі з дезінформацією та пропагандою, а також посиленні захисту критичної інфраструктури від кібератак.

У Стратегічному компасі ЄС (далі – «Стратегічний компас»), який Рада Європейського Союзу ухвалила 21 березня 2022 року – менше ніж через місяць після російського вторгнення в Україну – акцент було зроблено на посиленні стійкості держав і суспільств до інформаційних маніпуляцій та зовнішнього втручання в політичні процеси, а також на розширенні можливостей підтримки держав-членів у реагуванні на кризи, спричинені гібридними методами.

Цього має бути досягнуто за допомогою набору інструментів ЄС для протидії гібридним загрозам – «EU Hybrid Toolbox» (інструментарій EU Hybrid Toolbox (EUHT)), який має на меті зібрати всі цивільні та військові інструменти, які можна використовувати для протидії гібридним кампаніям.

Військова агресія з боку Росії проти Україні, яка триває з 2014 року, продемонструвала важливість скоординованого реагування для протидії гібридним кампаніям, наслідком яким можуть стати відкриті воєнні дії, має надати додатковий імпульс для досягнення ефективних результатів розробки EUHT.

1. Підхід ЄС до боротьби з гібридними загрозами.

У 2016 році Європейський Союз у своїй «Спільній структурі протидії гібридним загрозам» визначив гібридні з'явища як «поєднання репресивної та підривної діяльності з використанням традиційних і нетрадиційних методів (тобто дипломатичних, військових, економічних і технологічних), які можна використовувати спільно з державними та недержавними суб'єктами для досягнення конкретних цілей, тоді як ці дії є нижчими за поріг офіційно оголошеної війни» [1]. Вони можуть бути використані для досягнення різних

стратегічних, оперативних і тактичних цілей, спільним знаменником яких є дестабілізація держав-членів і всього ЄС, а також втручання в їхні політичні, соціальні та економічні процеси. Широкий підхід ЄС до цього питання є результатом специфіки самого явища, яке є складним, багатогранним і неоднозначним, а також відображає різні перспективи безпеки та пріоритети зовнішньої політики окремих держав-членів. Такий гнучкий підхід дозволяє врахувати загрози зі сходу (Росія, Білорусь) і півдня (Іран, терористичні організації, нелегальна міграція), а також загрози глобального масштабу (Китай).

Таким чином, було створено «Каталог гібридних методів і тактик», який включає: дезінформаційну та пропагандистську діяльність, кібератаки, втручання в політичні процеси (наприклад, вибори та референдуми), економічний тиск, інструменталізацію нелегальної міграції, державну підтримку збройних груп і найманців, розвідувальні операції підривного та диверсійного характеру, терористична діяльність або використання хімічних агентів, біологічних, радіологічних і ядерних.

З 2015 року ЄС відчуває ворожу гібридну активність, насамперед з боку Росії. У меншій мірі – але з явною тенденцією до зростання – такі методи використовують також Китай, Білорусь, Іран і Північна Корея, а також терористичні організації та радикальні кола.

Гібридні методи можуть використовуватися в різному обсязі та зі змінною інтенсивністю, а також можуть вільно комбінуватися державними чи недержавними агресорами, методи дій яких не є однаковими.

Крім того, відкритий каталог гібридних засобів бою, розширення якого, на думку інституцій ЄС, веде у тому числі до: загострення політичного суперництва за участю Росії (особливо після вторгнення в Україну) та Китаю, нестабільна ситуація в сусідстві ЄС і так звана «вепонізація» подальших секторів безпеки (наприклад, охорони здоров'я, клімату та навколишнього середовища).

Прикладом мілітаризації охорони здоров'я є російська та китайська кампанії дезінформації про вакцинацію та пандемію COVID-19. Екологічні проблеми можуть бути використані, щоб призвести до поляризації та соціального розколу в ЄС, а проблеми, пов'язані зі зміною клімату, можуть, у свою чергу, сприяти дестабілізації південних сусідів ЄС, міграційним кризам і зростанню ролі терористичних організацій. Інструменталізація цих явищ зовнішніми гравцями (наприклад, створення міграційних маршрутів або надихання радикалів на здійснення терористичних атак) становить пряму загрозу для країн ЄС. Каталог гібридних загроз також розширюють нові та проривні технології (Emerging disruptive technologies – EDT), включаючи розробку штучного інтелекту, які надають передові технічні можливості для проведення дезінформації, пропаганди, розвідки та підривної діяльності. Вищезазначені умови значно ускладнюють розробку процедур реагування на різні сценарії гібридних атак, оскільки загрози цього типу – через їх транскордонний та мережевий характер – вимагають комплексного та

багатовимірного підходу до раннього виявлення, запобігання та реагування на кризові ситуації.

З 2016 року ЄС нарощує можливості для протидії гібридним загрозам у чотирьох сферах:

1) підвищення обізнаності про ситуацію;

2) формування імунітету;

3) протидія та реагування на кризові ситуації (включаючи подолання їх наслідків);

4) співпраця та координація з партнерами та міжнародними організаціями (переважно НАТО).

«Стратегічний компас» закликає зміцнити ці можливості в рамках скоординованої відповіді ЄС на кризи, спричинені гібридними методами, і, перш за все, створити нові механізми та покращити ефективність їх використання. Тягар відповідальності за боротьбу з гібридними загрозами наразі лежить на органах національної безпеки (тобто секретних службах, поліції та армії), які мають відповідні юридичні та виконавчі повноваження (відповідно до статті 4(2) ДЄС).

«Стратегічний компас» не вносить жодних змін у цю сферу. Інструменти, створені в рамках «EU Hybrid Toolbox», для досягнення ефекту синергії та ефективнішого реагування мають надавати більшу підтримку національним зусиллям у боротьбі з гібридними загрозами та координувати спільні дії.

2. Ситуаційна обізнаність.

«Стратегічний компас» підкреслює важливість подальшого зміцнення розвідувальних можливостей ЄС для забезпечення обізнаності про ситуацію та прогнозування загроз. Особливе значення тут має створення механізмів обміну інформацією про гібридні загрози, зокрема, тому що така тактика є модусом дії переважно іноземних розвідувальних служб.

Підвищення обізнаності інституцій ЄС та держав-членів у цій сфері збільшить здатність ЄС швидко виявляти та реагувати на кризи, спричинені гібридними методами. Це також покращить координацію діяльності окремих країн. Роботу в цій сфері було розпочато у 2016 році зі створенням Відділу у справах синтезу інформації про гібридні загрози (Hybrid Fusion Cell) при Розвідувальному та ситуаційному центрі Європейського союзу (основний орган зовнішньої розвідки Європейського союзу, який об'єднує всі спецслужби країн союзу. Основною функцією є збір та аналіз інформації про діяльність іноземних організацій та громадян. Основний орган зовнішньої розвідки та контррозвідки Євросоюзу (EU INTCENT)) [2].

У ньому працюють цивільні та військові аналітики з Управління розвідки Військового штабу ЄС (EUMS), відповідальні за розробку звітів, брифінгів та аналізу гібридних загроз, що виникають у країнах ЄС та сусідніх країнах у рамках Єдиної системи аналізу розвідувальних даних (SIAC). Матеріали доступні для інституцій ЄС: Європейської ради (РЄ), Європейської комісії (ЄК), Європейської служби зовнішніх дій (ЕСЗД), Горизонтальної робочої групи з

посилення стійкості та протидії гібридним загрозам (ERCHT) та окремих держав-членів (через контактні пункти – у випадку Польщі це офіцер зв'язку Агентства внутрішньої безпеки при Постійному представництві Республіки Польща при ЄС). У дослідженнях використовується інформація як з відкритих, так і з закритих джерел, надана розвідувальними службами та службами безпеки держав-членів, агенцій ЄС (включаючи Європейський центр боротьби з кіберзлочинністю, Європейський центр боротьби з тероризмом і Frontex) і країн-партнерів (включаючи США, Канаду, Норвегія).

У частині виявлення загроз у кіберпросторі у роботі Відділу у справах синтезу інформації про гібридні загрози допомагають представники групи реагування на надзвичайні ситуації в комп'ютерних ситуаціях CERT-UE (Computer Emergency Response Team for the EU Institutions). Обмін конфіденційною інформацією, такою як технічні дані облікових записів, адміністраторів, програмне забезпечення або інфраструктура, що використовується для проведення операції з дезінформації, має вирішальне значення для можливості покласти відповідальність за цю діяльність на певну особу та накласти на неї санкції [3].

«Hybrid Fusion Cell» є ключовою установою, відповідальною за надання ситуаційної обізнаності установам ЄС та державам-членам. Його створення сприяло збільшенню потенціалу ЄС щодо раннього виявлення криз, спричинених гібридними методами, а також прискоренню та координації спільної відповіді держав-членів. Прикладом цього є реакція ЄС (у тому числі у формі ефективної стратегічної комунікації) на міграційну кризу на кордоні з Польщею, Литвою та Латвією, спричинену в середині 2021 року Білоруссю (за допомогою Росії), яка тривала кілька місяців [4]. Незважаючи на білорусько-російську дезінформаційну діяльність, спрямовану на розбіжності щодо тлумачення ситуації на кордоні [5], ЄС зберіг узгодженість і розцінив цю діяльність як гібридну атаку [6].

У березні 2019 року ЄС створив Систему швидкого оповіщення про дезінформацію (Rapid Alert System on Disinformation), яка мала на меті підвищення ситуаційної обізнаності щодо маніпулювання ворожою інформацією. Обмін інформацією в рамках цієї системи відбувається через контактні пункти, створені в окремих країнах ЄС – у випадку Польщі це спеціальний відділ стратегічної комунікації в Міністерстві закордонних справ, який займався переважно дезінформацією щодо пріоритетів польської зовнішньої політики.

Згадану Систему швидкого оповіщення про дезінформацію використовували у 2020 році під час пандемії COVID-19, коли інформаційний простір заполонила хвиля російської та китайської дезінформації, підриваючи довіру до західних вакцин (переважно мРНК), інституцій ЄС та стратегій вакцинації та підживлюючи рухи проти вакцинації [7]. Об'єктами атак тоді було, серед іншого, Європейське агентство з лікарських засобів. Система ЄС використовувалася для обміну інформацією між інституціями ЄС та

державами-членами, представниками приватного сектору, G7 та членами НАТО. Однак ці дії не зупинили поширення теорій змови, зокрема: групами проти вакцинації або проросійськими та прокитайськими новинними каналами (включаючи «фабрики тролів»).

3. Формування імунітету щодо дезінформації та пропаганди.

Побудова стійкості країн ЄС та їхніх суспільств – спрямована на зменшення сприйнятливості до ворожої дезінформації й пропаганди та на посилення захисту критичної інфраструктури від кібератак, тероризму, саботажу та диверсій. «Стратегічний компас» приділяє особливу увагу посиленню опору ЄС маніпулюванню іноземною інформацією та втручанню в політичні процеси.

Підхід ЄС до боротьби з маніпулюванням інформацією складається з чотирьох елементів, прийнятих Європейською Комісією в грудні 2018 року в Плані дій проти дезінформації (The Action Plan against Disinformation):

1) підвищення спроможності інституцій ЄС виявляти, аналізувати та розкривати дезінформацію;

2) посилення скоординованої та спільної відповіді на дезінформацію;

3) мобілізація приватного сектору для боротьби з дезінформацією;

4) підвищення обізнаності та покращення соціальної стійкості шляхом підтримки незалежної журналістики, ініціатив із перевірки фактів та сприяння медіа-освіті.

У відповідь на російські інформаційні та психологічні кампанії у 2015 р. в рамках Європейської служби зовнішньої діяльності (ЄСЗД) було створено робочу групу «East StratCom», яка мала відповідати за моніторинг, аналіз і реагування на російську пропаганду та дезінформацію. Спочатку колектив складався лише з трьох осіб, на даний момент у ньому 16 штатних співробітників. «East StratCom» стежить за випусками новин більш ніж 20 мовами. У першій половині 2022 року команда ідентифікувала майже 14 тис. випадків російської дезінформації, які були занесені в базу даних «EUvsDisinfo». Команда також проводить тренінги для персоналу з країн-партнерів, вживає заходів для зміцнення незалежної журналістики та поширює знання про ЄС та його політику в країнах Східного партнерства. Подібні завдання виконують аналогічні групи, створені в 2017 році (по шість штатних працівників кожна), відповідальні за регіон Західних Балкан (Western Balkans Task Force) і Близький Схід і Північну Африку (South Stratcom Task Force), які зосереджуються на протидії радикалізації. і боротьба з пропагандою терористичної діяльності організації, а також з дезінформацією з Росії, Китаю, Ірану та Туреччини.

Усі ці команди є частиною Відділу стратегічних комунікацій, робочих груп та аналізу Європейської служби зовнішньої діяльності, який підтримує інституції ЄС у плануванні політики, стратегій та інструментів стратегічної комунікації. Він також надає підтримку (наприклад, аналіз та інструкції щодо протидії дезінформації) дипломатичним місіям ЄС, місіям і операціям Спільної політики безпеки та оборони.

Ця структура також розвиває співпрацю з країнами-партнерами, G7, неурядовими організаціями, громадянським суспільством та приватним сектором (наприклад, у сфері збору даних за допомогою сучасного програмного забезпечення та технологій). Метою цих заходів є підвищення обізнаності громадськості та посилення опору країн-сусідів ЄС дезінформації.

За оцінкою ЄСЗД, російська дезінформація становить найбільшу загрозу для країн ЄС через її системний характер. Росія має достатні ресурси для проведення дезінформаційних кампаній, які є частиною довгострокової стратегії дестабілізації та дезінтеграції євроатлантичного регіону. Масштаби російської дезінформації набагато більші, ніж у країн, які наслідують Росію в цій сфері (наприклад, Китай). Однією з найбільш чутливих і сприйнятливих до дезінформації сфер функціонування країн ЄС є демократичні політичні процеси, такі як вибори та референдуми. У період з листопада 2016 року по квітень 2019 року втручання Росії в політичні процеси стосувалися 16 із 20 таких випадків у всьому світі (вони мали місце, зокрема, у Великій Британії, Франції, Німеччині та Іспанії) [8]. Вони набули переважно форми дезінформаційних кампаній і кібератак, зокрема: злом веб-сайтів і зміна їх вмісту, атака на виборчу інфраструктуру або викрадення та публікація інформації (злом і витік) з метою маніпулювання громадською думкою.

Щоб захистити виборців країн ЄС від дезінформації та кібернетичного втручання, група реагування на комп'ютерні надзвичайні ситуації ЄС «CERT-EU» створила спеціальний сервіс «Social Media Assurance», який дозволяє виявляти та видаляти облікові записи, які видають себе за профілі інших людей.

У вересні 2018 року ЄС також прийняв Кодекс практики, який регулює співпрацю між країнами ЄС і приватним сектором щодо зобов'язань онлайн-платформ і рекламної індустрії щодо підвищення прозорості політичної реклами та її фінансування, закриття фальшивих акаунтів і блокування. організації, відповідальні за дезінформацію. Кодекс був прийнятий, зокрема, найбільшими платформами онлайн-послуг, включаючи «Facebook», «Google», «Twitter» і «Microsoft». Ці дії були спрямовані на захист виборів до Європарламенту в травні 2019 року.

«Стратегічний компас» оголосив про створення нового механізму для підвищення ситуаційної обізнаності та стійкості ЄС, держав-членів та їхніх суспільств до маніпулювання інформацією та втручання в політичні процеси (Foreign Information Manipulation and Interference Toolbox, FIMI). Нова платформа співпраці спрямована на стандартизацію методів збору, аналізу та обміну даними (між урядами держав-членів, приватним сектором, громадянським суспільством і міжнародними організаціями) про тактику, методи та процедури, які використовують гібридні актори. Це посилить здатність ЄС виявляти та аналізувати кампанії з дезінформації на ранній стадії, полегшить збір доказів зовнішнього втручання в демократичні політичні процеси та стандартизує методи звітування про такі інциденти. Швидше за все, Центр аналізу та обміну інформацією (ISAC) буде створено в рамках «FIMI Toolbox» [9].

Укріплення імунітету щодо дезінформації та пропаганди країн ЄС також стосується таких ключових секторів, як кібербезпека, критична інфраструктура, енергетика, транспорт, оборона, фінансова система, безпека на морі та космос [10]. Ці зусилля зосереджені насамперед на створенні правових інструментів та здатності реагувати на інциденти та кризові ситуації, спричинені гібридними методами (особливо у кіберпросторі). Проривом у підході ЄС до кібербезпеки стало прийняття у 2016 році Директиви про безпеку мережевих та інформаційних систем (так звана Директива NIS). Документ зобов'язує держави-члени гарантувати мінімальні спільні стандарти кібербезпеки, зокрема: завдяки прийняттю національних стратегій кібербезпеки або створенню груп реагування на комп'ютерні інциденти, які працюватимуть у європейській мережі «Computer Emergency Response Team» (CERT). Директива також зобов'язала повідомляти про кіберінциденти ключових постачальників послуг у секторах енергетики, транспорту, банківської справи та фінансів, охорони здоров'я, водопостачання та цифрової інфраструктури. Крім регуляторної діяльності, ЄС, через Європейське агентство мережевої та інформаційної безпеки (ENISA) і Європейську організацію з кібербезпеки (ECSO) також підтримує дослідницьку діяльність і державно-приватну співпрацю. Спроможності держав-членів щодо кіберзахисту, у свою чергу, розвиваються за допомогою чотирьох проектів структурованої співпраці в рамках Permanent Structured Cooperation (PESCO), які стосуються обміну інформацією про кіберінциденти, координації дій, підтримки та спільного реагування, а також дослідження та навчання [11].

У грудні 2020 року Європейський Союз прийняв нову стратегію кібербезпеки [12], яка спрямована на підвищення стійкості держав-членів до кібератак і кращий захист критичної інфраструктури від них. Прикладом секторальних дій у цій сфері є набор інструментів кібердипломатії ЄС (EU Cyber Diplomacy toolbox).

У травні 2019 року було встановлено режим санкцій для реагування на кібератаки, скоєні проти країн, що не входять до ЄС, або з використанням інфраструктури, розташованої за межами Співтовариства. Суб'єкти, включені в «чорний список», відповідальні за або підтримують кібератаки проти країн ЄС, будуть піддані санкціям у вигляді заборони на в'їзд на територію ЄС або заморожування активів. Подібний режим санкцій запроваджено проти країн, які використовують хімічну зброю (в секретному списку 20 речовин), що є прямою відповіддю ЄС на використання російськими спецслужбами нервово-паралітичного газу «Новачок» на території Великобританії.

У 2019-2022 роках ЄС також надав фінансову підтримку в розмірі 11,6 млн євро Організації із заборони хімічної зброї (ОЗХЗ) для роботи, пов'язаної з протидією розробці та застосуванню хімічної зброї.

4. Протидія та реагування на кризи.

«Стратегічний компас» ЄС підкреслює важливість посилення спроможності Європейського Союзу реагувати на кризи, спричинені

гібридними методами. Було оголошено про створення до кінця 2024 року Груп швидкого гібридного реагування ЄС (EURHRTs), завданням яких буде підтримка держав-членів під час таких атак. Ці групи, швидше за все, також будуть використовуватися в рамках місій та операцій ЄС, а також для надання допомоги країнам-партнерам. Хоча робота над створенням EURHRTs знаходиться на концептуальній стадії, ці групи, швидше за все, будуть побудовані за моделлю Counter-Hybrid Support Teams (CHST) [13], створеної у 2018 році НАТО. Вони складаються переважно з цивільних експертів у сфері стратегічних комунікацій, кібербезпеки, контррозвідки, енергетичної безпеки та захисту критичної інфраструктури. У разі потреби вони також можуть бути розширені за допомогою військових радників. У кризовій ситуації вони можуть бути направлені в державу-член (на її запит) або діяти як консультативна група у створенні національних оборонних структур для протидії гібридним загрозам.

5. Важливість співпраці з НАТО

Стратегічний компас наголошує на важливості співпраці у боротьбі з гібридними загрозами з партнерами, зокрема: G7, ООН і НАТО. У цьому відношенні ЄС відводить ключову роль своїм відносинам з Північноатлантичним альянсом.

Антигібридна стратегія, ухвалена НАТО в 2015 році, складається з трьох елементів:

1) підготовка до гібридних атак шляхом збільшення можливостей розвідки та раннього попередження, посилення захисту критичної інфраструктури та тестування процесів прийняття рішень всередині Альянсу;

2) стримування (стримування) потенційного агресора шляхом застосування санкцій і тримання його в невизначеності щодо характеру відповіді;

3) захист (захист) союзників у разі гібридної агресії (особливо із застосуванням військових засобів) [14].

У деклараціях 2016 і 2018 років ЄС і НАТО розробили перелік із 74 спільних заходів безпеки, з яких понад 20 стосуються протидії гібридним загрозам. Вони зосереджені насамперед на розпізнаванні явища, підвищенні обізнаності про ситуацію, розбудові стійкості суспільства, захисті критичної інфраструктури та реагуванні на кризові ситуації, спричинені гібридними методами. Обидві організації працюють над реалізацією спільних ініціатив, використовуючи систематичні (неформальні) механізми співпраці між співробітниками на трьох взаємопов'язаних рівнях:

1) експертному,

2) проміжному (в рамках Основної групи ЄС-НАТО) і 3) стратегічному (керівний ЄС-НАТО). Група).

Завдяки неформальній співпраці організації розробили загальний операційний протокол (збірник ігор) для обміну знаннями про гібридні дії та координації відповідей. Разом вони чітко поставили собі за мету зробити протидію гібридним загрозам пріоритетом ЄС.

Першою спільною ініціативою ЄС і НАТО щодо протидії гібридним загрозам стало створення Європейського центру передового досвіду з протидії гібридним загрозам (Hybrid CoE) у Гельсінкі у 2016 році. Вказана структура служить аналітичним центром, експертно-консультативною підтримкою та платформою для обміну досвідом та інформацією щодо гібридних загроз. Центр у Гельсінкі, в першу чергу, сприяє підвищенню ситуаційної обізнаності обох організацій, так само як EU Hybrid Fusion Cell або її еквівалент НАТО Hybrid Analysis Branch, що працює в Об'єднаному відділі розвідки та безпеки (JISD). Обидві структури мають налагоджені робочі контакти завдяки щомісячному обміну персоналом. Аналітичні підрозділи ЄС і НАТО з гібридних загроз також готують спільні оцінки загроз (паралельні та скоординовані оцінки). Подібна співпраця також розвивається між East StratCom Task Force і Центром передового досвіду зі стратегічних комунікацій НАТО (StratCom CoE) у Ризі, які розробляють, серед іншого, спільні навчальні матеріали, а також курси реагування на дезінформацію для співробітників ЄС і НАТО.

У практичному вимірі Гельсінський центр відповідає за організацію семінарів, семінарів і навчань, наприклад, моделювання засідань Північноатлантичної ради (NAC) і Комітету з політики безпеки (PSC) під час гібридних атак. З 2017 року ЄС і НАТО паралельно та скоординовано проводять навчання EU Integrated Resolve і NATO Crisis Management Exercise (CMX) (Parallell and Coordinated Exercises (PACE), метою яких є перевірка здатності реагувати на кризи (включаючи гібридні) на основі спільного операційного протоколу.

Організації також шукають можливості для спільної (додаткової) відповіді на загрози в кіберпросторі, зокрема: спільні тренування та навчання (наприклад, Cyber Phalanx, Locked Shields або NATO Cyber Coalition), обмін інформацією та доктринальними документами, регулярні робочі контакти та освітні проекти. Ця співпраця відбувається, серед іншого, через Європейське оборонне агентство (EDA) і Центр передового досвіду кіберзахисту НАТО в Таллінні.

Іншим важливим елементом є співпраця в технологічному вимірі, включаючи обмін досвідом і практиками між CERT-EU та NATO Computer Incident Response Capability (NCIRC), які діють при Верховному командуванні об'єднаних сил у Європі (SHAPE).

6. Слабкі сторони підходу ЄС до боротьби з гібридними загрозами.

Рішення інтегрувати антигібридні інструменти ЄС у «EU Hybrid Toolbox» є кроком у правильному напрямі, особливо з огляду на постійне збільшення гібридної активності Росії, Китаю та інших гравців. Однак «EU Hybrid Toolbox» не вирішує всіх проблем слабких сторін ЄС в цій сфері. По-перше, «Стратегічний компас» прямо не вказує на можливість застосування положення про солідарність (стаття 222 Договору про функціонування Європейського Союзу) або положення про взаємну оборону (стаття 42(7) Договору про Європейський Союз) у разі гібридної атаки проти держави-члена.

Оскільки під час кризи агресор намагається порушити єдність ЄС і НАТО та паралізувати їхні процеси прийняття рішень, для зменшення ризику такого сценарію необхідні ширша дискусія, моделювання та навчання щодо використання обох пунктів.

Наразі країни ЄС можуть застосувати положення про солідарність, яке зобов'язує інших членів спільноти надавати допомогу у разі терористичного нападу, природного чи техногенного лиха. Вони можуть зробити це, звернувшись із запитом безпосередньо до Голови Ради та Президента Європейської Комісії через Координаційний центр реагування на надзвичайні ситуації (ERCC) лише після того, як національні та європейські варіанти реагування будуть вичерпані та якщо вони виявляться недостатніми для стримування криза. Окремі держави-члени самостійно приймають рішення щодо характеру допомоги та обсягу підтримки. Допомога має ґрунтуватися на принципах узгодженості та взаємодоповнюваності та на основі Інтегрованого реагування на політичні кризи ЄС (ICPR). Його координує Рада у співпраці з Європейською комісією, ЄСЗД та Верховним представником (з урахуванням їх повноважень). Існуючі (галузеві) інструменти реагування (політичні, фінансові та операційні), прийняті, серед іншого, для цілей боротьби з тероризмом, захисту критичної інфраструктури або кіберпростору, можуть використовуватися, серед іншого, у відповідь на кібератаки та підривну та диверсійну діяльність, інспіровану зовнішніми акторами.

Через неоднозначність гібридних загроз (наприклад, труднощі з визначенням суб'єкта, відповідального за атаку), оцінку обґрунтованості застосування положення про солідарність було доручено Високому представнику та ЄК (у межах їх компетенції), що поширюється на час реакції та дає агресору простір для втручання в процес прийняття рішень (у тому числі через дезінформаційну діяльність).

Чітка вказівка на те, що держави-члени можуть застосувати положення про солідарність у разі гібридних загроз, матиме значні політичні наслідки та слугуватиме стримуючим фактором. Це також ускладнило б супротивнику маніпулювання оцінкою ситуації окремими країнами ЄС.

Щоб було активовано положення про взаємну оборону (ст. 42 розділ 7 Договору про Європейський Союз), яке зобов'язує членів ЄС надавати підтримку державі ЄС, що стала жертвою збройної агресії, гібридні дії повинні здійснюватися з використанням військових засобів або ряд із них (наприклад, кібератаки на критичну інфраструктуру) – мають далекосяжні наслідки та дають підстави визнавати ці дії збройною агресією [15].

Гібридні операції, за своєю природою, проводяться за порогом війни, що створює ризик неодностайного тлумачення і, як наслідок, зволікання чи бездіяльності. Тому невідомо, як ЄС відреагує, наприклад, на серію диверсійно-диверсійних операцій проти збройового сектору, продукція якого постачається в Україну, і чи буде така подія вважатися агресією.

Варто, однак, зазначити, що ст. 42 розділ 7 Договору про Європейський Союз – єдиний раз в історії ЄС – на який Франція застосувала після терактів 2015 року. Країни ЄС одностайно підтримали Францію, хоча це була внутрішня загроза, а не зовнішня збройна агресія. Рішення застосувати положення про взаємний захист замість положення про солідарність було насамперед символічним і політичним. Залишається відкритим питання, чи відповість ЄС подібним чином на гібридну атаку, спрямовану, наприклад, проти країни з меншим потенціалом і значенням в ЄС, і які саме дії будуть тоді вжиті [16].

Робочі напрями ЄС вказують на те, що гібридні атаки некінетичної природи (наприклад, у кіберпросторі) можуть стати основою для запуску положення про взаємодопомогу. Про це свідчать, серед іншого навчання з реагування на кібератаки, проведені в дусі ст. 42 розділ 7 Договору про Європейський Союз. Принципи співпраці у цій сфері між державами-членами та окремими інституціями ЄС сформульовані в Рекомендації щодо скоординованої реакції на масштабні кіберінциденти та кризи. У ньому, серед іншого, було наголошено на: ключове значення ситуаційної обізнаності для ефективної координації на технічному (зміцнення безпеки мереж та IT-систем), операційному (обмін інформацією), а також стратегічному та політичному рівнях.

Не менш важливо, що «Стратегічний компас» не розробив військово-політичних механізмів для реагування на повномасштабний збройний конфлікт (якому передують ворожі гібридні дії), таким чином залишивши ключову роль НАТО у забезпеченні спроможності колективної оборони.

Оскільки членство Фінляндії та Швеції в НАТО зменшило кількість країн ЄС поза структурами НАТО до чотирьох (Австрія, Кіпр, Ірландія, Мальта), ініціативи щодо розвитку можливостей колективної оборони ЄС, ймовірно, будуть послаблені на користь розвитку кризових засобів управління. Це має зміцнити європейський стовп Альянсу та взаємодоповнюваність обох організацій у вимірі безпеки та оборони. «Стратегічний компас» оголосив про створення так званих Засобів швидкого реагування (RDC) чисельністю 5000 солдатів і складається з компонентів, які обслуговують певну місію чи операцію ЄС. Вони будуть призначені, насамперед, для виконання завдань, що випливають зі ст. 43 Договору про Європейський Союз, тобто діяльність з роззброєння, гуманітарні та рятувальні місії, військові консультації та підтримка, запобігання конфліктам, підтримка або відновлення миру, а також операції зі стабілізації в постконфліктний період.

RDC також слід використовувати для підтримки держав-партнерів, яким загрожує конфлікт або нестабільність у результаті ворожої гібридної діяльності.

Висновки з даного дослідження і перспективи подальших досліджень. Створення інструментів «EU Hybrid Toolbox» посилить можливості Європейського Союзу протидіяти гібридним загрозам і реагувати на них. Комплексний антигібридний інструментарій, розроблений у 2016 році, характеризується гнучкістю реагування та відкритістю до нових гібридних

методів і тактик, що використовуються як державними, так і недержавними структурами.

Тягар реагування на ворожі гібридні дії лежить на державах-членах (відповідно до статті 4(2) Договору про Європейський Союз), тоді як роль ЄС полягає в їх підтримці та координації спільних реакцій на кризові ситуації. Впровадження нових інструментів і методів роботи збільшиться, серед іншого: обізнаність про ситуацію та стійкість інституцій ЄС, держав-членів та їхніх суспільств, особливо проти маніпулювання інформацією та іноземного втручання в демократичні процеси.

Проте «EU Hybrid Toolbox» був би ефективнішим інструментом, якби він краще інтегрував розподілений набір інструментів ЄС (політичних, оперативних, інформаційних і фінансових) для боротьби з гібридними загрозами. Щоб спростити державам-членам використання цих інструментів, ЄС міг би прийняти єдиний документ (наприклад, оновлену загальну структуру чи стратегію), який об'єднує та організовує антигібридні інструменти та чітко визначає розподіл ролей, завдань і повноважень між інститути ЄС. Щоб зміцнити потенціал реагування ЄС, держави-члени повинні також ініціювати обговорення можливості застосування положення про солідарність або взаємодопомогу у випадку гібридних криз.

Завдяки багатосторонній співпраці розвідки, створенню гібридної термоядерної клітини та системи раннього попередження проти дезінформації, Союз значно покращив свою обізнаність про ситуацію. Складність гібридних загроз та очікуване збільшення кількості секторів, сприйнятливих до вепонізації (включно з безпекою здоров'я, зміною клімату, захистом навколишнього середовища та новими технологіями), породжують потребу посилити аналітичні можливості цих структур – збільшити кількість персоналу та фінансові ресурси.

В інтересах України є поглиблення співпраці з цими структурами через дипломатичних та військових представників. Це дозволить отримати доступ до європейського досвіду щодо протидії гібридним загрозам.

Створення нових інструментів розпізнавання дезінформаційних кампаній і втручання в політичні процеси (FIMI) та реагування на гібридні кризи (EURHRT) знаходиться лише на концептуальній стадії. «Стратегічний компас» також не уточнює, з яких саме елементів вони складатимуться і за яких умов їх можна використовувати.

Підхід ЄС до боротьби з гібридними загрозами зосереджується лише на їхньому невійськовому вимірі (тобто дезінформація, пропаганда, кібератаки), недостатньо розвиваючи військові можливості для реагування на використання повного спектру гібридних методів (включно з військовими чи парамілітарними).

ЄС має розглянути, якою може бути роль RDC під час гібридної кризи на території держав-членів (наприклад, інструменталізація міграції, терористична чи диверсійно-диверсійна діяльність або проникнення на територію озброєних груп). Їх превентивне розміщення (наприклад, у разі кризи на зовнішньому кордоні ЄС) стало б чітким сигналом агресору про те, що подальша ескалація

ситуації зустрінеться рішучою відповіддю ЄС. Ці дії мають здійснюватися в консультаціях з НАТО, на основі взаємодоповнюваності обох організацій і зміцнення європейської опори Альянсу.

ЄС має також чітко вказати на можливість застосування положення про солідарність (у разі масштабної та значної гібридної кризи) або положення про взаємодопомогу (у разі використання військових або воєнізованих гібридних методів). Це підвищило б безпеку держав-членів, які могли б розраховувати на одночасні та узгоджені дії як ЄС, так і НАТО. Неоднозначність гібридних дій (зокрема, наприклад, складність їх віднесення до конкретного суб'єкта) створює ризик різного тлумачення кризової ситуації, подовження процесів прийняття рішень в ЄС, а отже, уповільнення або неадекватність відповідь. Їх можна звести до мінімуму, серед іншого: шляхом розробки рішень за допомогою моделювання та навчань, що проводяться як всередині ЄС, так і у співпраці з НАТО на основі реальних сценаріїв гібридних криз. Вони також повинні враховувати можливі майбутні форми атак з використанням нових методів і тактик.

Стаття надійшла до редакції 05.10.2023 р.
Стаття рекомендована до друку 20.11.2023 р.

Hranovskyi M. V.,
Department of Political Science and Philosophy
Educational and Scientific Institute «Institute of Public Administration»,
V. N. Karazin Kharkiv National University,
4, Svobody Sq., Kharkiv, 61022, Ukraine,
e-mail: granowski_m@ukr.net https://orcid.org/0000-0002-8554-7456

MODERN MECHANISMS USED BY THE EU TO COMBAT HYBRID THREATS

Annotation. In today's world, there is a trend towards a significant increase in the number of hybrid conflicts, which are becoming more and more sophisticated and unpredictable.

The article is devoted to the analysis of practical mechanisms for countering hybrid threats, including from state authorities, in particular, in the EU countries.

The modern practice of hybrid operations on the part of the aggressor demonstrates a radical change in the tactics and means used by a state-player of the world level against an adversary that is weak and unable to protect the integrity of its own territory.

The beginning of the XXI century. is characterized by new challenges in the field of international security. It is believed that the end of the "Cold War" did not eliminate internal or regional sources of conflicts and did not ensure stable peaceful coexistence of countries in the world. According to experts, the international community is faced not so much with a direct armed conflict, but with one of the varieties of military operations, which can also be called hybrid.

Keywords: security, hybrid warfare, hybrid conflict, hybrid actions, hybrid operations, terrorism.

REFERANCES

1. Joint Framework on countering hybrid threats a European Union response. (2016). *European Commission. Brussels. 6 kwietnia 2016 r.* URL: https://eur-lex.europa.eu [in Polish].

2. Pełną zdolność operacyjną Komórka osiągnęła w .połowie 2017 r.

3. E. Kaca. (2021). Możliwości wprowadzenia sankcji UE za kampanie dezinformacyjne. *Biuletyn PISM, nr. 104 (2302), 26 maja 2021 r.* URL: www.pism.pl [in Polish].

4. A.M. Dyner. (2022). Kryzys graniczny jako przykład działań hybrydowych. *PISM Strategic File, nr. 2, luty 2022*. URL: www.pism.pl [in Polish].

5. F. Bryjka, A. Legucka. (2021). Dezinformacja i propaganda Rosji oraz Białorusi w kontekście polsko-białoruskiego kryzysu granicznego. *Biuletyn PISM, nr. 212 (2410), 9 grudnia 2021 r*. URL: www.pism.pl [in Polish].

6. European Council conclusions of 21 and 22 October 2021. URL: www.consilium.europa.eu/media/52622/20211022-euco-conclusions-en.pdf [in Polish].

7. A. Legucka, M. Przychodniak. (2020). Dezinformacja Chin i Rosji w trakcie pandemii COVID-19. *Biuletyn PISM", nr. 86 (2018), 21 kwietnia 2020 r*. URL: www.pism.pl [in Polish].

8. Hacking democracies Cataloguing cyber-enabled attacks on elections. *Australian Strategic Policy Institute.* URL: www.aspi.org.au

9. 2021 StratCom activity report - Strategic Communication Task Forces and Information Analysis Division. 24 marca 2022 r. URL: www.eeas.europa.eu

10. A. Kozioł. (2022). Kmpas Strategiczny: w stronę unijnej koncepcji bezpieczeństwa i obrony kosmosu. *PISM Policy Paper, nr. 1, styczeń 2022*. URL: www.pism.pl [in Polish].

11. P. Szymański. (2020). NATO i Unia Europejska wobec zagrożeń hybrydowych. *Komentarze OSW, nr. 328, 24 kwietnia 2020 r.* URL: www.osw.waw.pl [in Polish].

12. The EU's Cybersecurity Strategy for the Digital Decade. 16 grudnia 2020 r. URL: https://digital-strategy.ec.europa.eu

13. CHST są instrumentem reagowania NATO na zagrożenia hybrydowe poniżej progu art. 5 Traktatu północnoatlantyckiego, który dotyczy zbiorowej obrony. Dotychczas CHST wykorzystano dwukrotnie: w 2019 r. w Czarnogórze (w związku z cyberatakami i dezinformacją w okresie wyborczym) oraz w 2021 r. na Litwie (w związku z kryzysem migracyjnym na granicy z Białorusią).

14. NATO's response to hybrid threats. 16 marca 2021 r. URL: www.nato.int

15. Zob. Resolution on the mutual defence clause (Article 42(7) TEU). 2015/3034(RSP). 21 stycznia 2016 r. URL: https://oeil.secure.europarl.europa.eu

16. W 2015 r. państwa UE zgodziły się na wsparcie operacji antyterrorystycznych w Syrii, Iraku i Sahelu.

The article was received by the editors 05.10.2023.
The article is recommended for printing 20.11.2023.