I. Desiatnikov

UNITED STATES - VIETNAM RELATIONS IN LIGHT OF GEOPOLITICS OF THE USA IN ASIA-PACIFIC REGION IN 1945-1975

The article focuses on the analysis of US-Vietnam relations during the period from 1945 to 1975. The aim of the article is to trace the changes that took place in the US-Vietnam relationship over that period, to identify the factors that influenced them, as well as the approaches used by the heads of the countries to tackle their foreign policy objectives in the region.

The author traces the evolution of US policy in Vietnam pursued by Presidents H. Truman, D. Eisenhower, J. Kennedy, L. Johnson and R. Nixon. The United States had diametrically opposed position on relations with the Vietnamese governments, namely, confrontation and military conflict with the Democratic Republic of Vietnam, and cooperation, military and economic aid to the Republic of Vietnam.

The author concludes that the US attitude towards Vietnam was determined by the international situation at that time, including the beginning of the Cold War. The policies of Presidents D. Eisenhower and J. Kennedy were to restrain the expansion of the Communist bloc's sphere of influence. The direct involvement of the US military in the Vietnam conflict, initiated by L. Johnson, pursued the goal of enhancing the prestige of the United States in the global confrontation with the USSR.

The split between the Soviet Union and China was used by the US to get out of the Vietnam War and mend relations with China as a counterweight to the Soviet Union in the Asia-Pacific region. Instead, the Republic of Vietnam, which had been the "junior partner" of the United States, was left to its fate.

Keywords: *United States of America, Democratic Republic of Vietnam, Republic of Vietnam, interstate relations, Asia-Pacific region.*

УДК 32.019.51:070.16(4-672ЄС)

Л. Дорош

ВІДПОВІДЬ НА ГІБРИДНІ ЗАГРОЗИ: ОСОБЛИВОСТІ СТРАТЕГІЇ ЄВРОПЕЙСЬКОГО СОЮЗУ У БОРОТЬБІ З ДЕЗІНФОРМАЦІЄЮ

Проаналізовано особливості комплексної стратегії Європейського Союзу у боротьбі з дезінформацією. Прослідковано, що для реагування на гібридні загрози у рамках ЄС функціонують такі інструменти – «Оперативна робоча група зі стратегічних комунікацій», «Координаційна група з питань гібридних загроз» та «Система швидкого оповіщення». Стверджується, що використання багаторівневого, крос-секторального підходу дає можливість ЄС поступово нарощувати його захисні сили у протидії модерним гібридним загрозам. Наголошено, що Україні, яка потерпає від гібридної війни, вкрай важливо залучати досвід використання окремих інструментів, вироблених у рамках ЄС, у боротьбі з дезінформацією та забезпечення стійкості до гібридних викликів.

Ключові слова: *гібридна війна, дезінформація, Європейський Союз, Оперативна робоча група зі стратегічних комунікацій, Координаційна група з питань гібридних загроз, Система швидкого оповіщення*.

DOI 10.34079/2226-2830-2020-10-27-106-116

Посилення гібридних загроз глобального та регіонального рівнів вимагає зміцнення безпекового потенціалу Європейського Союзу. Сьогодні ці загрози стали основним центром уваги для політиків, чиновників, аналітиків та дослідників у ЄС. Ці загрози трактуються як критичні. Саме на підготовку відповіді на них спрямована спільна діяльність держав Європи. У рамках ЄС країни-члени спільно випрацювали Спільну зовнішню політику та політику безпеки (СЗППБ) (Common Foreign and Security Policy (CFSP), спільну політику безпеки та оборони (СЗПБ) (Common Security and Defence Policy (CSDP)), Зону свободи, безпеки та справедливості (the Area of Freedom, Security and Justice (AFSJ) та Безпековий Союз (Security Union). ЄС підштовхнули до таких дій головно агресивна поведінка Росії та захоплення Криму у 2014 році. У об'єднані побоюються, що Росія може використовувати ту саму тактику щодо інших колишніх радянських республік та членів Варшавського договору. Крім того, занепокоєння викликають дії Даєш в південному сусідстві ЄС, що змусили Об'єднання звернути увагу на особливості використання соціальних медіа та мереж для радикалізації європейців та спрямування терористичних операцій на європейському континенті. Нарешті, кібератаки, ініційовані з Китаю чи Ірану, підривні операції комерційних структур (наприклад, Wannacry та NotPetya), дезінформаційні кампанії не лише порушили критичну інфраструктуру в Європі, але й послабили довіру до європейських демократичних інститутів та процесів (наприклад, діяльність Cambridge Analytica) [16]. У такому випадку для подолання таких гібридних викликів ЄС повинен не тільки захищати свої інституції від зовнішніх державних суб'єктів, а й від внутрішніх загроз, що йдуть від політичних груп у межах її держав-членів [22].

ЄС сьогодні вкрай серйозно сприймає гібридні загрози і розробляє механізми протидії їм. Тут йдеться про кризи, що тривають за його межами, на його східних та південних кордонах. Як в Україні, так і інших країнах ЄС намагається протидіяти головно ворожим діям Росії, окрім цього реагує на активність США та Китаю, а також на використання нових технологій, таких як 5G. Однак контрзаходи ЄС передусім зосереджені на внутрішньому вимірі його розвитку, враховуючи, що держави-члени ЄС передусім піддаються гібридним атакам. Ці заходи в цілому допомагають «забезпечити майбутнє» самого ЄС, створити його внутрішні структури й мережі в умовах швидкозмінюваного міжнародного ландшафту. Таке зміцнення безпекових структур передбачає передусім творення інституцій на наднаціональному рівні, а також узгодження спільного для європейського простору інструментарію протидії безпековим викликам.

Одним із ключових інструментів у гібридній війні стала дезінформація в Інтернеті – поширення неправдивої або оманливої інформації на веб-платформах для впливу на громадськість. Такий інструмент у повній мірі використовує Росія у гібридній війні проти України, а також для впливу на суспільства західних демократій. ЄС заявляє, що «дезінформація спотворює істину, відволікає від істини і відкидає істину», вона стає «зброю для впливу на громадську думку, створення та посилення поділів у суспільстві та підриву довіри до державних установ та виборчих систем» [11]. ЄС визнає ці загрози та реагує на них, розробляючи комплексну стратегію боротьби з дезінформацією, створюючи відповідні інститути та творячи відповідну нормативно-правову базу, викриваючи неправдиві повідомлення та зміцнюючи незалежні ЗМІ.

Мета цього дослідження – комплексно проаналізувати стратегію та інституційну структуру ЄС, що спрямована на протидію гібридним впливам у інформаційній сфері.

Джерельну базу цього дослідження становлять головно документи ЄС [1-2; 4-9] та інформація про діяльність структур ЄС, створених для протидії дезінформації [3; 10; 19]. Також міцну основу цього дослідження склали довідкові та публіцистичні матеріали [11-13; 15; 18], у яких досліджуються сучасні виклики у сфері подолання кіберзагроз, протидії дезінформації, забезпечення кібербезпеки тощо. Варто також викормити аналітичні роботи Д.Файота та Р.Паркса [16], С. Столтона [19-20], К.Торінгтон [22], які зосереджують увагу на інституційній структурі, виробленій у рамках ЄС, діяльність якої спрямована на протидію сучасним гібридним викликам та захист Європи.

Важливо розуміти, що безпекова архітектура ЄС стосується не лише її військової компоненти. Тут йдеться, окрім іншого, й про безпеку європейської цифрової економіки, кібербезпеку, безпеку морської, космічної та енергетичної сфер. До них слід додати й такі надважливі сектори, як безпека кордонів ЄС, захист його критичної інфраструктури та інформаційного середовища. Захист останніх трьох сфер означає захист наріжних каменів самого Європейського Союзу, без них неможлива подальша інтеграція європейської економіки та розвиток демократичних інститутів, що її підтримують [16]. Отож, у нашому дослідженні акцентуємо увагу на комплексному з'ясуванні специфіки інституційного та інструментального забезпечення безпеки Об'єднання у сфері подолання гібридних загроз, враховуючи, що таких захист має міжінституціональний характер і охоплює різноманітні сфери.

У червні 2016 р. Верховний представник Союзу з питань зовнішньої політики та політики безпеки та віце-президент Європейської комісії оприлюднили Глобальну стратегію ЄС (EU Global Strategy). Її ключовою тезою є «захист Європи» - через управління кризами, захист кордонів та зусилля по боротьбі з екстремізмом, кібератаками та дезінформацією через «зв'язок» між внутрішньою та зовнішньою безпекою. «Гібридна книга ЄС» («EU Hybrid Playbook») заклала основи для системи координації на рівні ЄС та на національному рівні у разі гібридної атаки [9]. Усі заходи, вжиті ЄС з 2015 р., були підсумовані 12 червня 2018 р. у звіті про виконання спільної платформи щодо протидії гібридним загрозам («Report on the implementation of the joint framework on countering hybrid threats») та 26 червня 2018 р. у спільному повідомленні про підвищення стійкості та протидії гібридним загрозам («Communication on increasing resilience and bolstering capabilities to address hybrid threats») [7] та запропоновано подальші дії у цій сфері. І, нарешті, 5 грудня 2018 р. ЄС опублікував свій план дій щодо подолання дезінформації («Action Plan against disinformation») [5], що передбачає встановлення партнерських відносин між структурами ЄС, державами-членами та онлайн-платформами.

Загалом дослідники виділяють 10 заходів, які здійснює ЄС для протидії дезінформації:

1. Створення публічної бази даних EuvsDisinfo (2015 р.), метою якої є підвищення рівня обізнаності громадськості та розуміння випадків дезінформації, а також допомога громадянам розвивати опір цифровій дезінформації та маніпуляціям у ЗМІ.

2. Захист виборів у ЄС (захист персональних даних, прозорість політичної реклами в інтернеті, посилення кібербезпеки), наголошуючи, що забезпечення стійкості демократичних систем Союзу є частиною «Безпекового Союзу».

3. Розвінчування єврміфів. ЄС розробив серію спеціалізованих кампаній у кількох країнах ЄС, розвінчуючи національні варіанти міфів, пов'язаних з функціонуванням ЄС.

4. Моніторинг дезінформаційний повідомлень системою швидкого оповіщення (Rapid Alert System), яка дозволяє інституціям ЄС та державам-членам обмінюватись ідеями щодо подолання дезінформаційних кампаній, та координувати дії з їх відсічі.

5. Прийняття загальноєвропейського кодексу практики щодо дезінформації («EU-wide Code of Practice on Disinformation») спільно з онлайн-платформами. Провідні інтернет-компанії, такі як Google, Mozilla, Facebook, Twitter та Microsoft, підписали цей Кодекс, зобов'язавшись застосовувати більш жорсткі правила та вказівки щодо поширення дезінформації, видаляти фейкові облікові записи та забезпечувати прозорість поширення політичної реклами.

6. Організація заходів, що сприяють посиленню медіаграмотності. Тут йдеться про проведення щорічного Європейського тижня медіаграмотності (European Media Literacy Week), що охоплює понад 320 заходів, що сприяють посиленню медіаграмотності в Європі. Європейська комісія також підтримує такі проекти, як детектори брехні (Lie Detectors), які спонукають школярів до критичного мислення.

7. Посилення ролі громадянського суспільства у виявленні та викритті дезінформації. ЄС заохочує громадські організації виявляти та викривати дезінформацію в Інтернеті. Однією з таких ініціатив є волонтерський проект «Keyboard Warriors» у Польщі.

8. Посилення роботи платформ з перевірки фактів (fact-checkers) шляхом інвестування у їх діяльність. ЄС інвестує у нові технології, що пов'язані із перевіркою змісту і відслідковуванням поширення дезінформації в соціальних медіа (до прикладу, веб-платформа «Truly Media», розроблена спільно Афінським технологічним центром (Athens Technology Center) та Deutsche Welle).

9. Здійснення кампаній, які сприяють підвищенню обізнаності громадян щодо негативних наслідків дезінформації. У Єврокомісії стверджують, коли громадяни знають про позитивний вплив політики та цінностей ЄС на їх повсякденне життя, вони також стають більш стійкими до негативних наслідків дезінформації. За допомогою комунікаційних кампаній, таких як InvestEU, EUandMe та EU Protects, ЄС інформує громадян про їхні права та про те, як він захищає їх від дезінформації.

10. Підтримка свободи та плюралізму ЗМІ для забезпечення здорової демократії. ЄС поважає свободу та плюралізм ЗМІ, а також право на свободу вираження поглядів. Дезінформацію можна подолати, підтримуючи незалежних журналістів та журналістів-розслідувачів, які продукують високоякісний новинний матеріал [11].

Загалом для реагування на гібридні загрози у рамках ЄС функціонують такі інструменти – «Оперативна робоча група зі стратегічних комунікацій» (East StratCom Task Force (ESTF), «Координаційна група з питань гібридних загроз» (Hybrid Fusion Cell (HFC) та «Система швидкого оповіщення» (Rapid Alert System – Disinformation (RAS-DIS). Аналітики зазначають, що бюджет на 2019 рік для цих структур зріс з 1,9 мільйона євро у 2018 році до 5 мільйонів євро. Крім того, передбачається розширення кількості співробітників команди стратегічної комунікації впродовж найближчих двох років, а саме експертів з пошуку та аналізу даних [22].

У 2015 р. у рамках ЄС створено «Східну групу StratCom» (East StratCom Task Force) для боротьби з дезінформацією російських урядових та провладних медіа-джерел, що спрямована проти держав Європи та держав Східного партнерства (Вірменія, Азербайджан, Білорусь, Грузія, Молдова та Україна) [1]. Ця група була створена ще до виборів у США у 2016 р., з метою кращого реагування на спроби Кремля вплинути на виборців та зруйнувати європейську єдність. Особливо це наголошувалось щодо колишніх радянських республік

[14]. Згодом вплив російських груп було підтверджено і щодо референдуму по Брекзіту, і щодо виборів у Франції та Німеччині. Відтак, така протидія має довгострокові виміри.

У діяльності групи наголошується на значенні стратегічного спілкування, розробці комунікаційних продуктів та кампаній, що орієнтовані на краще пояснення політики ЄС у країнах Східного партнерства. Діяльність робочої групи здійснюється у рамках більш широких зусиль ЄС, спрямованих на зміцнення медіа-середовища в регіоні Східного партнерства, у тісній співпраці з іншими членами ЄС. Цільова група повідомляє і аналізує тенденції дезінформації, пояснює та розкриває дезінформаційні повідомлення та сприяє підвищенню обізнаності про дезінформацію, що надходить з російських державних медіа ресурсів, проросійських джерел та поширюється у медіапросторі політики сусідства [19]. Переважно такі комунікаційні стратегії були орієнтовані на країни Східного партнерства. Пізніше були створені такі ж спеціальні групи з питань стратегічної комунікації для Півдня та Західних Балкан.

У згаданому нами Плані дій проти дезінформації [5] ЄС визнав, що ESTF каталогізувала, проаналізувала та поставила у центрі уваги понад 4500 прикладів дезінформації, що використовується Російською Федерацією, розкривши численні повідомлення про дезінформацію, підвищивши обізнаність та викривши інструменти, методи та наміри дезінформаційних кампаній.

Важливого значення ЄС надає підвищенню рівня обізнаності та створенню спеціальних механізмів для обміну інформацією з країнами-членами та координації спроможності ЄС щодо реалізації стратегічних комунікацій. 6 квітня 2016 р. ЄС окреслив спільну основу щодо протидії гібридним загрозам, яка, серед іншого, передбачала створення центру «Координаційна група з питань гібридних загроз» («Hybrid Fusion Cell») для розвідки, збору інформації та аналізу потенційних гібридних загроз у розвідувальному та ситуаційному центрі ЄС («EU's intelligence and situation centre» (INTCEN) [4]. Метою функціонування такого інституту є отримання, аналіз та обмін інформацією, інформування осіб, які приймають рішення, як в установах ЄС, так і в державах-членах щодо індикаторів гібридних загроз та попередження щодо них [12]. Лише у координації з відповідними органами ЄС та на національному рівні Fusion Cell аналізуватиме зовнішні аспекти гібридних загроз, що впливають на ЄС та його сусідів, з метою швидкого аналізу відповідних інцидентів та інформування про стратегічні процеси прийняття рішень ЄС, у тому числі надання даних до оцінки безпекових ризиків на рівні ЄС. Група сприятиме зростанню поінформованості та робитиме вклад у процеси оцінки безпекових ризиків, які сприятимуть розробці політики на національному та європейському рівнях [15].

Система швидкого оповіщення (Rapid Alert System- Disinformation (RAS-DIS) є ще одним інструментом у загальній системі ЄС у боротьбі з дезінформацією та є одним із стовпів згаданого нами Плану дій проти дезінформації, затвердженого Європейською Радою у грудні 2018 р. Ця система є частиною інституцій ЄС, яка сприяє обміну думками щодо дезінформаційних кампаній та координує протидію їм у режимі реального часу. Над проектом працює близько 140 осіб, які діляться всіма повідомленнями, аналізами та звітами щодо випадків дезінформації. Також система включає вбудовану функцію оповіщення у випадку широкомасштабної дезінформаційної кампанії, на зразок кампанії у США у 2016 р. [17]. Діяльність RAS-DIS ґрунтується на загальнодоступній інформації, а також система повинна використовувати наукові дані, дані досліджень, платформ перевірок фактів, онлайн-платформ та міжнародних партнерів [19]. У її рамках передбачено створення Цільової цифрової платформи (Dedicated Digital Platform), у межах якої держави-члени та

інституції ЄС можуть ділитися інформацією та баченнями щодо дезінформації та координувати відповіді на них. Також перебачено функціонування мережі із 28-ми національних контактних пунктів, які координуватимуть участь урядів держав-членів ЄС та обмінюватимуться інформацією та кращими практиками в межах RAS-DIS. Потенційними результатами дії системи стануть заходи з інформування та підвищення обізнаності громадськості; збереження прикладів важливих випадків на веб-платформах; розширення можливостей дослідників, мереж перевірок фактів та громадянського суспільства; скоординована відповідь; скоординована залученість тощо.

Важливо відзначити, що ця система швидкого попередження про дезінформацію ініційована у 18 березня 2019 р., однак станом на жовтень 2019 р. ще у повній мірі не використовувалась. Ключовим поясненням цьому є, окрім іншого, невизначеність параметрів, за якими оцінюють міру впливу, шкідливість та масштаб кампанії з дезінформації. Тут йдеться про те, щоб виміряти, чи той чи інший випадок дезінформації є частиною більшої транскордонної кампанії, чи вона координується, здійснюється навмисно, з політичною метою та з конкретним аудиторним «охопленням» [20]. Відтак, джерела зазначають, що з часу запуску системи ЄС не виявив таку кампанію, яка була б порівнянна, наприклад, з кампанією, про яку повідомлялося під час президентських виборів у США. Однак, у ЄС розуміють, що якщо навіть не було виявлено дезінформаційних кампаній за допомогою таких інструментів, це не означає, що вони повністю відсутні [13; 17].

Систему швидкого оповіщення сьогодні критикують, як «нешвидку, несповісницьку, несистемну» [22]. Це важливо з точки зору відсутності ефективної співпраці з державами-членами, браку координаційної роботи поміж 28-ма національними урядами, які не мають власних систем моніторингу дезінформації. Відтак, за відсутності скоординованої діяльності ЄС у боротьбі з дезінформацією у всіх 28-ми державах-членах існує висока вірогідність, що у окремих країнах більш неконрольованіше поширюватимуться фейкові повідомлення. Чиновники ЄС зазначають, що у 2020 р. буде здійснено оцінку потенційної діяльності системи і буде прийнято рішення, чи вона функціонуватиме у рамках власного нормативного регулювання чи у рамках дії майбутнього Закону про цифрові послуги – нової правової бази, яка повинна бути представлена в 2020 р. [20].

Сьогодні RAS-DIS використовується ЄС для моніторингу серйозних випадків дезінформації після низки онлайн-кампаній, що стосуються спалаху коронавірусу у світі та Європі. У випадку виявлення фальшивих новин про коронавірус в Інтернеті, система поширює інформацію про дезінформацію між країнами-членами, а також партнерами з Великої сімки [21].

Погоджуємось з думкою аналітиків, які зазначають, що важливість цієї системи швидкого оповіщення не в тому, щоб фіксувати кількість виявлених оповіщень, а в тому, що держави-члени ЄС можуть вчитися одне в одного обміну даними та спільно оцінювати дезінформаційні кампаній, які мали успіх [19].

Слід зазначити, що ЄС розробив низку політичних ініціатив, які покликані допомогти Союзу та його державам-членам реагувати на гібридні загрози та підвищити власну стійкість й у сфері кібербезпеки. У 2013 р. ЄС оприлюднив стратегію кібербезпеки, а в 2016 р. було прийнято Директиву щодо безпеки мережевих та інформаційних систем по всьому ЄС («Directive on the security of network and information systems across the EU» – NIS Directive). Цю Директиву всі члени ЄС імплементували до 9 травня 2018 р. На додаток до кіберзахисних висновків Європейської програми з питань безпеки (European Agenda on Security) у 2015 р., ЄС представив спільне повідомлення під назвою «Опір, стримування та

оборона: розбудова сильної кібербезпеки для ЄС («Joint Communication entitled 'Resilience, Deterrence and Defence: Building Strong Cyber Security for the EU») [7], що включає такі ініціативи, як, наприклад, посилення Агентства ЄС з питань мережевої та інформаційної безпеки («EU Agency for Network and Information Security» (ENISA) та вироблення плану координованого реагування на масштабні інциденти та кризи в кібербезпеці в ЄС [2]. 6 лютого 2018 р. країни-члени ЄС погодились створити платформу «Освіта, навчання, тренінги та оцінювання» («Education, Training, Exercise and Evaluation (ETEE) platform») для координації діяльності у сфері кібербезпеки та підготовки та освіти в галузі кібербезпеки в межах ЄС. Ця платформа була запущена в листопаді 2018 р. після залучення експертів з окремих країн [3]. 4-8 червня 2018 р. були організовані спільні навчання із кіберзахисту «Cyber Phalanx 2018», які відбувались у формі імітаційних навчань, які проходили в місті Уолс-Зізенхайм (Австрія). 28 червня 2018 р. шість країн-членів ЄС (Австрія, Бельгія, Естонія, Фінляндія, Німеччина та Латвія) підписали Меморандум про об'єднання та обмін можливостями в галузі кібербезпеки, що має на меті організацію спільних навчань та посилення обміну інформацією [10]. 10 грудня 2018 р. Європейська Комісія вирішила посилити кіберспроможність Союзу шляхом створення Агенції ЄС з питань кібербезпеки («EU Agency for Cybersecurity»). Отож, ЄС надає особливого значення тренуванням та навчанням, дослідженням та залученням технологій, цивільно-військовому співробітництву та міжнародному співробітництву у цій сфері.

Однак зусилля ЄС не обмежуються лише кібербезпекою. ЄС підвів підсумки щодо імплементації спільної платформи щодо протидії гібридним загрозам та посилення практичного реагування на гібридні загрози [8]. Важливо відзначити, як уважно ставиться ЄС до практичної підготовки у сфері протидії гібридним загрозам. Так, у межах об'єднання було організовано низку навчань з посилення реагування на кризи. Слід зазначити, що ще в 2016 р. Європейське агентство з питань оборони (European Defence Agency (EDA)) організувало імітаційні навчання щодо вигаданої гібридної кризової ситуації. 28 вересня 2017 р. ЄС розпочав паралельні та скоординовані навчання (PACE17) за вигаданим сценарієм, щоб перевірити ситуаційну обізнаність ЄС, час реакції, канали комунікацій – та засвоїти деякі уроки. 30-31 січня 2018 р. Управління Європейської комісії з питань охорони здоров'я та безпечності харчових продуктів (the European Commission's DG for Health and Food Safety (DG SANTE) організувало міжгалузеві навчання з питань гібридних загроз (навчання «Химера») із використаням факторів пандемії. Такі тренування стали особливо актуальними у світлі використання отрути «Новічок» для отруєння у Солсбері, Великобританія. З 5 по 23 листопада 2018 р. було організовано великі цивільно-військові «Гібридні навчання ЄС 2018» (EU Hybrid Exercise 2018) (EU-HEX-ML 18). У ході цих навчань було залучено різні інституції та органи ЄС для розробки сценарію врегулювання кризи, із врахуванням різних аспектів зовнішньої та внутрішньої безпеки (гібридні атаки, енергетика, кібербезпека, охорона здоров'я, морська сфера тощо). Паралельно відбувались тренування під егідою НАТО у рамках програми Паралельних і координованих навчань (Parallel and Coordinated Exercise (PACE).

У січні 2020 р. European Union Task Force провели перший в історії саміт щодо ворожого зовнішнього впливу (головно з боку втручання східного сусіда – РФ та Китаю) У ході саміту обговорювались змінювані загрози, викликані поширенням дезінформації в середині ЄС, наголошувалось на необхідності вироблення крос-секторальної стратегії, спрямованої на боротьбу з дезінформаційнми кампаніями, картографування майбутніх загроз та діагностики сфер вразливості, а також визначення нових шляхів подолання цих

викликів. Чиновники ЄС наголошують на тому, що дезінформація поширюється щодо цілої низки питань, як-от міграція, сфера охорони здоров'я (особливо щодо пандемії короновірусу), зміна клімату та участі у виборчому процесі. У рамках саміту представники Європейської Комісії запропонували 2,5 мільйони євро для створення обсерваторії цифрових медіа, яка б об'єднала платформи перевірки фактів та наукових дослідників для боротьби з дезінформацією, і 60 мільйонів євро на 2021-2027 роки для підтримки якісної журналістики. З іншого боку, експерти стверджують, що сьогодні таких коштів є недостатньо [14].

Значення має й постійна співпраця з великими платформами соціальних мереж (Facebook, Twitter, Google, Microsoft, Mozilla), які взаємодіють у рамках Кодексу практики проти дезінформації («Code of practice against disinformation») та зобов'язані робити кроки для підвищення прозорості цих платформ, включаючи забезпечення прозорості політичної реклами у межах країн ЄС, співпрацю з платформами з перевірки фактів для виявлення дезінформаційного змісту (у тому числі пов'язаного з виборами), та видалення фальшивих облікових записів тощо [22]. Власне такі спільні зусилля та заходи у рамках спільного плану дій проти дезінформації, а також зусилля громадянського суспільства щодо підвищення обізнаності про загрози, сприяли стримуванню атак та викриттю дезінформаційного змісту, а отже, повинні тривати та поширюватись [14].

Слід зазначити, що сьогодні немає єдиновірного інструменту боротьби з дезінформацією та іншими гібридними впливами. Дослідники вказують на гібридну природу самого ЄС, що робить її незамінним фактором протидії гібридним загрозам [14]. Однак гібридний характер Союзу також робить його однозначно вразливим. Саме тому аналітики наголошують, що гібридні загрози вимагають обережної рівноваги між основними правами та безпекою, відкритим ринком та безпечною економікою. Окрім цього вони вимагають швидкості та рішучості, які у випадку ЄС часто недосяжні, через брак бажання та можливостей координації спільних зусиль державами-членами ЄС. Тут важливо також називати все своїми іменами (гібридну атаку – гібридною атакою), швидко реагувати та розвивати інституції як на наднаціональному рівні, так і на рівні країн-членів [16].

Висновуючи, слід зазначити, що ЄС, використовуючи баторівневий, крос-секторальний підхід, поступово нарощує свої захисні сили, зокрема стосовно модерних нетрадиційних загроз. Сучасні гібридні загрози не мають часових рамок, відтак, відповіді на них та зусилля з метою підвищення стійкості повинні стати перманентною особливістю зовнішньої та внутрішньої діяльності ЄС. Особливо важливо на сучасному етапі вчасно виявляти та усувати поточні виклики, слідкувати за новими вразливими ситуаціями та міжнародними акторами, для яких використання інструментів більш масштабної гібридної кампанії стало вже звичним. З іншого боку, слід погодитись з думкою аналітиків, що наразі ефективність заходів ЄС у протидії дезінформації є маловідомою та потребує детального вивчення, у тому числі із врахуванням факторів впливу внутрішнього та зовнішнього походження. Однак, слід розуміти, що створення та координація інституцій Об'єднання у цій сфері, вироблення політичних механізмів та прийняття стратегічних документів, вчасна та ефективна реакція ЄС – це ті кроки, які посилюють співтовариство. Україні ж, яка потерпає від гібридної війни, вкрай важливо залучати досвід використання окремих інструментів, вироблених у рамках ЄС, у боротьбі з дезінформацією та забезпечення стійкості до гібридних загроз.

Список використаної літератури

1. Action Plan on Strategic Communication [Electronic resource] // High Representative of the Union for Foreign Affairs and Security Policy. – 2015. –Ares(2015)2608242. – June 22. – Mode of access : http://archive.eap-csf.eu/assets/files/Action%20PLan.pdf

2. Commission Recommendation on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises [Electronic resource] // European Commission. – 2017. – C(2017)6100 final. – September 13. – Mode of access : https://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-6100-F1-EN-MAIN-PART-1.PDF

3. ESDC: Cyber platform for education, training, evaluation and exercise (ETEE) [Electronic resource] // EEAS. – 2018. – February 14. – Mode of access : https://eeas.europa.eu/headquarters/headquarters-homepage/39848/esdc-cyber-platform-education-training-evaluation-and-exercise-etee_en

4. Joint Communication establishing a Joint Framework on Countering Hybrid Threats // High Representative of the Union for Foreign Affairs and Security Policy. – 2016. – April 6. – JOIN(2017) 18 final.

5. Joint Communication on an Action Plan Against Disinformation [Electronic resource] // High Representative of the Union for Foreign Affairs and Security Policy. – 2018. – December 5. – JOIN(2018) 36 final. – Mode of access : https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf

6. Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats // High Representative of the Union for Foreign Affairs and Security Policy. – 2018. – June 13. – JOIN(2018) 16 final.

7. Joint Communication on Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU [Electronic resource] // High Representative of the Union for Foreign Affairs and Security Policy. – 2017. – September 13. – JOIN(2017) 450 final. – Mode of access : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=JOIN:2017:450:FIN&rid=3

8. Joint Report on the Implementation of the Joint Framework on Countering Hybrid Threats – A European Union Response // High Representative of the Union for Foreign Affairs and Security Policy. – 2017. – July 19. – JOIN(2017) 30 final.

9. Joint Staff Working Document: EU Operational Protocol for Countering Hybrid Threats – ‘EU Playbook // High Representative of the Union for Foreign Affairs and Security Policy. – 2017. – July 5. – SWD(2016) 227 final.

10. Six Member States agree to pool and share cyber ranges capabilities [Electronic resource] // European Defence Agency. – 2018. – June 28. – Mode of access : https://www.eda.europa.eu/info-hub/press-centre/latest-news/2018/06/28/six-member-states-agree-to-pool-share-cyber-ranges-capabilities

11. 10 actions that the EU undertakes to fight disinformation [Electronic resource] // Soma. – 2019. – September 24. – Mode of access : https://www.disinfobservatory.org/10-actions-that-the-eu-undertakes-to-fight-disinformation/

12. A Europe that protects: good progress on tackling hybrid threats [Electronic resource] // European Commission. – 2019. – 29 May. – Mode of access : https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2788

13. Dervey S. The EU’s Rapid Alert System: what are the results? [Electronic resource] / S. Dervey // EU Policies. – 2019. – October 30. – Mode of access : http://eu-policies.com/competences/economy/digital-economy/eus-rapid-alert-system-results/

14. European Union Task Force holds its first summit on fighting russian disinformation [Electronic resource] // Institute Mass Information. – 2020. – January 31. – Mode of access: https://imi.org.ua/en/news/european-union-task-force-holds-its-first-summit-on-fighting-russian-disinformation-cnn-i31479

15. FAQ: Joint Framework on countering hybrid threats [Electronic resource] // European Commission. –2016. – 6 April. – Mode of access : https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_1250

16. Fiott D. Protecting Europe. The EU's response to hybrid threats [Electronic resource] / D. Fiott, R. Parkes // Chaillot Paper. – 2019. – 151. – Mode of access : https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_151.pdf

17. Nielsen N. No large-scale disinformation detected in EU this year [Electronic resource] / N. Nielsen // Euobserver. – 2019. – 29 Oct. – Mode of access : https://euobserver.com/justice/146461

18. Questions and Answers about the East StratCom Task Force [Electronic resource] // European External Action Service. – 2018. – 05 December. – Mode of access : https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en

19. Rapid Alert System strengthening coordinated and joint responses to disinformation [Electronic resource]. – Mode of access : https://eeas.europa.eu/sites/eeas/files/ras_factsheet_march_2019_0.pdf

20. Stolton S. EU mulls disinformation regulation but admits alert system has 'never been triggered' [Electronic resource] / S. Stolton // Euractiv. – 2019. – 29 Oct. – Mode of access : https://www.euractiv.com/section/digital/news/eu-mulls-disinformation-regulation-but-admits-alert-system-has-never-been-triggered/

21. Stolton S. EU Rapid Alert System used amid coronavirus disinformation campaign [Electronic resource] / S. Stolton // Euractiv. – 2020. – 4 March. – Mode of access : https://www.euractiv.com/section/digital/news/eu-alert-triggered-after-coronavirus-disinformation-campaign/

22. Thorington K. Europe's Elections: The Fight Against Disinformation [Electronic resource] / K. Thorington // Council on Foreign Relations. – 2019. – May 23. – Mode of access : https://www.cfr.org/blog/europes-elections-fight-against-disinformation

L. Dorosh

RESPONSE TO HYBRID THREATS: PECULIARITIES OF THE EUROPEAN UNION STRATEGY ON COUNTERING THE DISINFORMATION

The features of the European Union's comprehensive strategy on countering the disinformation have been analyzed. It is emphasized on the creation of the legal framework and the activities of institutions aimed at countering the hybrid challenges, combating disinformation, exposing false messages and strengthening of the independent media. 10 actions of the EU to tackle the disinformation have been analyzed, such as creating the EuvsDisinfo public database, protection the integrity of EU elections, debunking Euromyths, monitoring disinformation messages with the Rapid Alert System, establishing the EU-wide Code of Practice on Disinformation, organizing events that promote media literacy, empowering civil society to both identify and expose disinformation, facilitating the work of fact-checkers, creating campaigns that raize public awareness on the disinformation's negative effects, supporting media freedom and pluralism for a healthy democracy. The instruments of the EU in response to the hybrid threats

such as the East StratCom Task Force (ESTF), the Hybrid Fusion Cell (HFC) and the Rapid Alert System - Disinformation (RAS-DIS) have been monitored. It has been determined that the EU is particularly attentive to practical training in combating hybrid threats. It is alleged that the use of a multilevel, cross-sectoral approach enables the EU to gradually increase its defence to counter modern hybrid threats. It is highlighted that Ukraine, which is suffering from the hybrid war, should involve the experience of the use of the instruments developed within the EU, adopting and sharing experience in combating disinformation and provide the resistance to hybrid challenges.

***Keywords**: hybrid war, disinformation, European Union, East StratCom Task Force, the Hybrid Fusion Cell, Rapid Alert System - Disinformation.*

УДК 327.7:316.647.82-055.2

М. В. Здоровега,
О. Я. Івасечко

СПЕЦИФІКА ДІЯЛЬНОСТІ МІЖНАРОДНИХ НЕУРЯДОВИХ ОРГАНІЗАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ ПРИНЦИПУ ГЕНДЕРНОЇ РІВНОСТІ: ДОСВІД ДЛЯ УКРАЇНИ

У статті розглядається специфіка діяльності міжнародних неурядових організацій щодо забезпечення принципу гендерної рівності. Увагу акцентовано на практиці діяльності таких міжнародних неурядових організацій, як-от: «Gender and Development Network» (GADN), Equality Now, Promundo, котрі безпосередньо виконують місію адвокації інтересів жінок, гарантування їхніх рівних можливостей з чоловіками у всіх сферах суспільного життя. Зроблено висновок про те, що в Україні відповідно до Звіту із глобального гендерного розриву за 2020 р. прослідковується позитивна динаміка у порівнянні з аналогічним звітом за 2014 р., однак найгіршою залишається ситуація із політичною компонентою (участю жінок у процесі прийняття рішень) – 83 місце із значенням, яке майже наближається до нуля, тобто, до суцільної гендерної нерівності.

***Ключові слова:** міжнародні неурядові організації, принцип гендерної рівності, Україна, глобальний гендерний розрив.*

DOI 10.34079/2226-2830-2020-10-27-116-126

Сьогодні для українського суспільства на порядку денному гостро постала не лише проблема «двополюсності суспільства» тобто поділ його на багатих та бідних, і фактично відсутність середнього класу (за окремими підрахунками середній клас в Україні складає 3 – 5 %), але і його стратифікація за цілим рядом ознак, з-поміж яких – стать, вік, соціальний статус чи клас, регіон проживання, стан здоров'я, сексуальна орієнтація, етнічна або національна, а також релігійна приналежність, тип населеного пункту тощо. З огляду на це, що в Конституції України фіксується твердження про те, що Україна – демократична країна, то необхідністю є повага та гідна репрезентованість інтересів та потреб різних соціальних груп (незалежно від їх розміру) у різних сферах суспільного життя, оскільки це – фундамент демократичного суспільства. Попри те, слід констатувати і той факт, що невід'ємним компонентом поняття рівності та рівних можливостей є гендерна рівність. Відтак, справді