УДК 351:354.1:327.8
DOI https://doi.org/10.32782/2786-5681-2023-4.07

Володимир БОНДАР
доктор філософії, професор кафедри економіки, підприємництва, менеджменту економічного факультету, Київський міжнародний університет
ptc.charit@gmail.com
ORCID: *0000-0002-9833-9867*

ТРАНСФОРМАЦІЯ ЗОВНІШНІХ АКТОРІВ ЗА СУЧАСНОГО ГІБРИДНОГО СВІТОУСТРОЮ

Анотація. Мета *статті полягає в дослідженні сучасних тенденцій проявів активності зовнішніх акторів через призму концепції гібридної війни.*

У статті обговорено основні терміни в контексті розгортання гібридного світоустрою з акцентом на поведінку зовнішніх акторів із застосування інформаційних засобів, її форми та методи в умовах технологічного прогресу. На прикладі проведеного західними експертами аналізу досвіду влади США з протидії кампанії дезінформації, організованої прокремлівськими акторами 2016 року під час президентських виборів, систематизовано ознаки проявів зовнішніх акторів. З'ясовано ключові компоненти інформаційного впливу, зміст прикладних рекомендацій фахівців на адресу американської виконавчої та законодавчої влади. Встановлено змінність фактора перспективи учасників гібридного протистояння, його актуальність для країни-об'єкта агресії. Через розуміння напрямів проведення інформаційного впливу в соціальних мережах наголошено про нові тенденції диверсифікації країною-агресором організаційних форм та спеціалізації суб'єктів у порівнянні з традиційною моделлю поведінки зовнішніх акторів, притаманною для міжнародної системи відносин. Відзначено роль спеціальних служб країни-ініціатора з формування мережі акторів.

Наукова новизна *статті полягає в тому, що застосуванням термінології гібридної війни в дослідженні реалізації зовнішніми акторами інформаційного впливу вперше продемонстровано важливість врахування фактора перспективи у сфері державного управління країною, яка стала об'єктом гібридного нападу, у напрямі організації протидії, реалізації зовнішньополітичного курсу.*

Практична значимість *статті пов'язана з можливістю подальшого теоретичного дослідження її основних положень і висновків при розробці методичних рекомендацій із проблематики сучасних трансформацій інформаційного впливу зовнішніх акторів відносно системи національної безпеки України, впровадження їх у навчальний процес, плануванні та реалізації управлінської діяльності ключових стейкхолдерів, передусім сектору безпеки, органів із регулювання інформаційного середовища, цифрового та медіапростору в напрямі протидії агресору. Окремого аналізу потребує фактор перспективи, його врахування в державному управлінні та публічній політиці.*

Ключові слова: *зовнішній актор, інформаційні засоби, інформаційний вплив, фактор перспективи, національна безпека.*

Volodymyr BONDAR
Doctor of Philosophy, Professor at the Department of Economics, Management, Business of the Faculty of Economics, Kyiv International University
ORCID: *0000-0002-9833-9867*

TRANSFORMATION OF EXTERNAL ACTORS IN A MODERN HYBRID WORLD ORDER

Abstract. *The* ***purpose*** *of the article is to study the current tendencies of manifestations of external actors through the prism of the hybrid war concept.*

The article discusses the basic terms in the context of the development of a hybrid world order with an emphasis on the behavior of external actors on the implementation the discourse means, its forms and methods in the conditions of technological progress. On the example of Western experts, the analysis of the US authorities' experience to response disinformation campaign by pro-kremlin actors in 2016 during the presidential election, the signs of external actors' manifestations were systematized. The major components of information influence, the content of applicate recommendations of experts to the US executive and legislative power have been clarified. The variability of the perspective factor of the hybrid confrontation participants, its relevance for the country-objective of aggression is established. Through understanding the directions of information influence in social networks, new trends in the use of organizational forms and specialization of subjects in comparison with traditional model of the external actors' behavior, which is inherent to international system of relations. The role of special services of the country-initiator of information influence on the formation of a network of actors is noted.

*The **scientific novelty** of the article, by use of hybrid war terminology in study of providing by external actors the information influence, for the first time it demonstrated the importance of taking into account the perspective factor in public administration by the country, which became the object of hybrid attack, in the direction of organizing a response, realization an international political course.*

*The **practical importance** of the article is related to the possibility of further theoretical study of its basic provisions and conclusions in the development of methodological recommendations regarding problems of modern transformations of information influence by external actors in relation to the national security system of Ukraine, their introduction into the educational process. Planning and implementation of management activities of key stakeholders, first of all, of security sector, regulation bodies of information, digital and media space in the direction of response to an aggressor. A separate analysis requires the perspective factor and its consideration in public administration and public policy.*

***Key words**: external actor, information means, information influence, perspective factor, national security.*

Постановка проблеми. За прийняту у вітчизняному науковому дискурсі відправну точку розгортання гібридного світового устрою стала агресія рф проти України з тимчасовою анексією Криму, окупацією українських східних територій. Від 24 лютого 2022 року змінюється парадигма сприйняття країнами Заходу, що поряд з об'єктністю нашої держави як головної арени російського гібридного нападу статус окремих із них трансформується зі спостерігача на об'єкт реалізації інформаційних засобів, а цілями стають їхні політичні інститути та публічний простір.

У сучасній реальності, як відзначається ключовими стейкхолдерами сектору безпеки Європи, зокрема Данії та Швейцарії, а також у Заяві глав держав-учасників Вільнюського саміту НАТО, з боку російських розвідувальних служб зафіксовано активізацію нелегальної та деструктивної діяльності; поширення кампанії дезінформації; формування мережі прокремлівських акторів у інформаційному, цифровому та медіапросторі на території європейських юрисдикцій; спроби незаконного проникнення до баз даних європейських операторів із великими масивами чутливої інформації [1; 2; 3].

Адаптацією провідних демократій до викликів відносно системи національної безпеки став перегляд концептуальних підходів регулювання інформаційної сфери, модернізація інституційних та організаційних механізмів. До прикладу, Єврокомісією внесено зміни до чинного Кодексу (2018 р.) прийняттям «Доповненого кодексу боротьби з дезінформацією» (2022 р.); Закону про цифрові послуги (2000 р.) − акту «Про єдиний ринок цифрових послуг та доповнення Директиви 2000/31/ЄС» (2022 р.). Законодавчо сформовано єдиний європейський ринок онлайн-провайдерів послуг затвердженням «Переліку великих онлайн-платформ та онлайн-пошукових систем» (2023 р.), передбачено механізми його регулювання. У євроатлантичному вимірі за результатами домовленості між США та ЄС щодо впорядкування обміну даних та їхнього захисту, відповідно до Регламенту Європейського Парламенту та Європейської Ради (2016 р.) прийнято акт «Адекватний рівень захисту персональних даних у рамках конфіденційності даних ЄС-США» (2023 р.). Поряд із цим режимом КНР з 1-го липня 2023 року запроваджено обмеження доступу нерезидентів до даних, що циркулюють на внутрішньому китайському ринку, у рамках удосконалення законодавства з протидії спеціальним службам іноземних держав, а також з метою підвищення рівня обізнаності населення, працівників ЗМІ та сфери культури [4]. В Індії 14-го серпня 2023 року президентом підписано відповідний закон про захист персональних даних, згідно з яким будь-які дії з обробки даних громадян дозволяються виключно за рішенням судових органів [5].

Еволюція технологічного сектору та утворення інформаційного простору без географічних кордонів слугують основою вдосконалення інструментарію та диверсифікації напрямів впливу зовнішніх акторів, спеціалізація яких усе більше зміщується в цифрову сферу інформаційних технологій. Для України, з точки зору фактора перспективи як держави-об'єкта гібридної агресії, важливо симетрично розвивати потенціал і спроможність протидії всупереч політичним цілям противника через адаптування до нових викликів.

Аналіз останніх досліджень та публікацій. В основу статті покладено наукові праці вітчизняних дослідників процесів формування гібридного світоустрою, безпекового середовища, розвитку понятійно-категоріального апарату концепту «гібридна війна», таких, як: О. Бодрук, М. Вавринчук, В. Горбулін, О. Їжак, О. Неклеса, В. Олуйко, Б. Парахонський,

О. Пошедін, М. Розумний, Г. Ситник, М. Требін, А. Шевцов, В. Яблонський, Г. Яворська. У розкритті предмета дослідження використано теоретичні розробки також таких зарубіжних авторів: Ф. Гоффмана, Т. Гюбера, Дж. Кеннана, В. Немета, П. Померанцева, Б. Ренза, А. Реча, Дж. Розенау, Г. Сміта, Р. Уолкера.

Мета статті – дослідити сучасні тенденції проявів активності зовнішніх акторів через призму концепції гібридної війни.

Виклад основного матеріалу. Концептуалізація терміна «*гібридна війна*» сприяє розумінню структури засобів, якими досягаються стратегічні політичні цілі: економічні, інформаційні, мілітарні, квазімілітарні, дипломатичні, інші немілітарні [6, с. 20]. За М. Трубіним, який, досліджуючи даний феномен, визначає інформацію як один з основних видів зброї війни шостого покоління, що застосовується агресором на стадії інформаційної боротьби для свідомого руйнування духовного світу цілих націй чи народів сторони-жертви [7]. Погоджуємося, інформація є основою діяльності різних форм поводження з нею: генерування, здобування, зберігання, захист, обробка, розповсюдження, інші. Тому одне з теоретичних та практичних завдань − як зовнішній актор застосовує інформаційні засоби з метою нейтралізації шкідливого впливу.

Колективом монографічної праці «Світова гібридна війна: український фронт» (2017 р.) сформована думка щодо принципового значення фактора перспективи для розуміння гібридної війни. Посилаючись на сучасну історію, вітчизняні дослідники виокремлюють три перспективи відносно подій залежно від ролі сторін конфлікту: агресор, об'єкт гібридного нападу, спостерігач [6]. На нашу думку, врахування перспективи є вкрай важливим для об'єкта нападу. Цінність захисту державного суверенітету, територіальної цілісності та оборони державних кордонів безумовна, але необхідною умовою є наявність національних ресурсів і можливість їх відновлення. Отож однією з імовірностей стабілізації стану системи національної безпеки, пріоритетним для об'єкта стає визначення позиції та політики іншого учасника-спостерігача: чи підтримуватиме він постраждалу сторону, якої інтенсивності й розміру ця допомога може бути. Інший важливий чинник для об'єкта – ідентифікувати статус іншої країни або групи країн, які також стали об'єктом гібридного нападу з метою організації спільних заходів із протидії дезінформації, узгодження управлінських рішень широкого спектра державної та публічної політики.

Певної уваги потребує термін «*актор*». У політологічному словнику представлено таке трактування: «Активний учасник (колективний чи індивідуальний) міжнародних відносин й світової політики, який, завдяки наявності в його розпорядженні актуальних та потенційних ресурсів і здатності їх ефективно використовувати, володіє можливостями самостійно, відповідно до власного розуміння своїх інтересів, приймати рішення і реалізовувати стратегію, яка здійснює істотний і тривалий вплив на міжнародну систему, що визнається як такий іншими учасниками та враховується ними при прийнятті власних рішень» [8]. Загальною класифікацією укладачі словника поділяють акторів на *державні* (створені суверенними державами міжнародні організації, державні інститути та інституції, місцевого самоврядування) та *недержавні* (неурядові організації, транснаціональні корпорації, політичні партії, громадські та релігійні організації, соціальні групи, інші утворення) [8]. Слушно модернізувати цей перелік, додавши сучасні прояви форм недержавних акторів, передусім це технологічні компанії; публічні діячі, політики, ексдипломатичні посадовці, науковці; аналітичні, консалтингові центри; ЗМІ, медіа. Не можна оминути спеціальні служби, проте, з огляду на непублічний характер діяльності їхня роль опосередкована утворенням суб'єктів або залученням існуючих, походженням (національні, міжнародні чи третьої юрисдикції).

Обговорюючи предмет дослідження, ми звертаємо нашу увагу на оцінку експертів США прокремлівської кампанії дезінформації навколо президентських виборів 2016 року. Основні висновки – це, по-перше, неготовність американських державних інституцій і медіа до такого виду інформаційного впливу; по-друге, спроможність акторів іншої країни проводити інформаційні акції під прикриттям для маніпулювання громадською думкою через соціальні мережі. Проведене ними визначення компонентів дало змогу виокремити три ключових: наявність «*маніпулятивного актора*», його «*оманлива поведінка*» та «*шкідливий зміст*» повідомлень.

Систематизуємо стисло сутність кожного з компонентів, виходячи з аналізу західних експертів. «*Маніпулятивний актор*» уособлює суб'єкт, який свідомо залучається до кампанії дезінформації та чітко розуміє свою роль, факт участі в ній. Необхідною умовою є приховування сутності й мети кампанії, маскування ідентичності актора. Завдяки можливостям інформаційно-технологічних засобів, в основі проведення лежить так званий принцип «гри в кішки-мишки» задля уникнення ідентифікації актора, який приховано маніпулює інформаційними засобами; стримування його активності в соціальних мережах на певному етапі реалізації для вдосконалення стратегії, якщо значна ймовірність ідентифікації. «*Оманлива поведінка*» передбачає застосування широкого діапазону інструментів та технік соціальних медіа для змістовного наповнення контенту, таких, як армії ботів (автоматизовані) чи ферми тролів (анонімні). З метою підвищення потужності порівняно меншого числа акторів, що беруть участь у кампанії, треба забезпечувати значимий ефект, якщо б вона реалізовувалася за більшої кількості акторів, але традиційним способом. «*Шкідливий зміст*» − цей компонент покликаний удосконалювати зміст на регулярній основі. Оскільки, у порівнянні з двома розглянутими вище компонентами, є найбільш прозорим і передбачає, що будь-який користувач спроможний формувати власну думку. На відміну від більш складного виклику для пересічного користувача, необхідно застосовувати відсутні в нього професійні навички або кваліфікацію, ідентифікувати ознаки прихованого характеру маніпулятивного актора, його оманливої поведінки.

Виходячи з практики, існують прикладні рекомендації експертів для американських законодавчих і виконавчих інституцій такого змісту: 1) кожен компонент має ключове значення, утім аналіз досвіду протидії владних органів показує, що за пріоритетністю найбільші зусилля спрямовуються в бік нейтралізації саме шкідливого змісту. Тому виникає потреба в збалансованому підході для аналізу як маніпулятивних акторів – нерезидентів чи резидентів, а їхня оманлива поведінка впливає на хід кампанії дезінформації; 2) кожному компоненту притаманний винятковий набір інформаційних засобів, напрямів впливу, компромісів, наслідків. Таким чином, викликом постає питання, як ефективно розподілити функціональні обов'язки та сфери компетенції між ключовими стейкхолдерами сектору безпеки, а також інформаційного, цифрового та медіапростору. Недостатньою буде політика або заходи протидії лише одному компоненту; 3) у сукупності компоненти «*маніпулятивні актори*» й «*оманлива поведінка*» спільно утворюють інформаційну асиметрію по відношенню до тих, хто намагається протистояти їхньому впливові. Звідси – необхідність усебічного аналізу інформаційних засобів та заходів протидії [9].

Спираючись на аналіз і теоретичні напрацювання, доходимо висновку, що політичні інститути Сполучених Штатів Америки стали безпосередньою метою покладання впливу прокремлівських акторів з метою формування сприятливої для режиму рф політичної кон'юнктури. Беручи до уваги період початку агресії проти України від 2014 року, втручання у 2016 році через кампанію дезінформації в процес формування президентської вертикалі США напередодні широкомасштабної агресії 2022 року, це дає підстави говорити про розширення росією комплексної гібридної агресії до масштабу світової гібридної війни. Із військовою та інформаційною фазою безпосередньо в Україні, а на території США та інших демократій − її інформаційною складовою. Припустивши, що політика з фінансової та військової допомоги атлантичного союзника України не змінюватиметься за нинішнього очільника від демократичної партії, а наступні президентські вибори відбудуться у 2024 році, то попереду можемо очікувати застосування інформаційних засобів у гібридній війні рф проти США ще більшої інтенсивності. Підсумок наступний: якщо раніше до обговорених вище подій фактор перспективи США вказував на їх роль переважною мірою як спостерігача конфлікту, то за нинішніх умов політичний устрій і публічний простір цієї країни являє собою повноцінний об'єкт зовнішнього інформаційного впливу з боку акторів російського режиму.

Завершуючи дискусію, можемо говорити про те, що з відходом від парадигми біполярного світу до багатополярного в умовах геополітики, по-перше, диверсифікуються організаційні форми акторів, що виводить їх за межі міжнародної системи відносин за рахунок

соціальних мереж до світового публічного простору. Інформаційний, цифровий і медіапростір перетворюються апріорі на арену застосування інформаційних засобів високої інтенсивності. По-друге, підмінюються соціальні цінності – на заміну світовому порядку, завдяки збалансованому механізму домовленостей чи компромісів між акторами, одна зі сторін конфлікту нівелює авторитет іншої сторони як суб'єкта та свідомо в односторонньому порядку діє на користь лише власних інтересів, у такий спосіб трансформуючи суб'єкт-суб'єктну взаємодію на ієрархічну модель «домінанта-меншість», за якої, за посередництвом інформаційних засобів, сторона-меншість перетворюється ініціатором-домінантою гібридної агресії з суб'єкта на об'єкт. По-третє, технологічний прогрес уможливлює значне розширення кола акторів залученням країною-агресоркою до проведення інформаційного впливу поряд безпосередньо з національними суб'єктами також опосередковано й суб'єктів походження з третьої юрисдикції, країни-об'єкта, країни-спостерігача. По-четверте, інтенсифікується діяльність спеціальних служб країни-ініціатора інформаційного впливу із залучення акторів модернізацією інформаційних засобів.

Висновки та пропозиції. У сучасному гібридному світоустрої відбувається трансформація напрямів інформаційного впливу зовнішніх акторів через соціальні мережі за рахунок розширення бази залучення суб'єктів інших, у порівнянні з традиційними формами учасників міжнародних відносин, організаційних структур і спеціалізацій. Технологічний розвиток сприяє застосуванню акторами більш різноманітних інформаційних засобів, високої інтенсивності. Однією і особливостей є активізація, на прикладі росії, спеціальних служб із формування мережі прокремлівських акторів за рахунок національних, іноземних чи міжнародних суб'єктів для залучення їх до проведення заходів інформаційного впливу. Іншою – відхід країною-агресоркою від збалансованих механізмів взаємодії до ієрархічної соціальної орієнтації. З точки зору фактора перспективи, важливо враховувати країною-об'єктом статусність інших країн-учасників конфлікту задля планування та реалізації політики протидії.

Перспективні наукові розвідки щодо подальшого теоретичного осмислення всього комплексу сутнісних характеристик зовнішніх акторів, напрямів гібридного нападу та видів інформаційних засобів, що застосовуються агресором; планування та реалізації протидії інформаційному впливу на дестабілізацію системи державної безпеки України з урахуванням нового гібридного світоустрою; модернізації механізмів державного управління та їх адаптації відповідно до фактора перспективи України як об'єкта гібридного нападу співвідносно до подібного фактора інших країн.

ЛІТЕРАТУРА:

1. Denmark warns of Russian spies posing as "journalists or business people". May 5, 2023. URL: https://therecord.media/denmark-russian-spies-warning-journalists-business-people

2. Vilnius Summit Communiqué issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Vilnius 11 July 2023. URL: NATO – Official text: Vilnius Summit Communiqué issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Vilnius 11 July 2023.

3. Бондар В.Т. Сучасні виклики в європейському безпековому середовищі: вплив на систему національної безпеки України : зб. матер. Міжнар. наук.-практ. конф. «Національна безпека України в умовах сучасних викликів» (м. Чернігів, 22 серпня 2023 року). Чернігів : ГО «Науково-освітній інноваційний центр суспільних трансформацій», 2023. С. 7–10. DOI: https://doi.org/10.54929/conf_22_08_2023-01-01

4. Multinationals in China accelerate push to decouple data. July 16, 2023. URL: https://archive.ph/df4Wr

5. The Digital Personal Data Protection Bill. *Ministry of Electronics and Information Technology.* 2023. New Delhi, India. URL: https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023

6. Світова гібридна війна: український фронт : моногр. / за заг. ред. В.П. Горбуліна. Київ : НІСД, 2017. 496 с.

7. Требін М.П. «Гібридна» війна як нова українська реальність. *Український соціум*. 2014. № 3(50). С. 113–127.

8. Політологічний енциклопедичний словник / уклад. Л.М. Герасіна, В.Л. Погрібна, І.О. Поліщук та ін. ; за ред. М.П. Требіна. Харків : Право, 2015. 816 с.

9. François C. Actors, Behaviors, Content: A Disinformation ABC. Highlighting Three Vectors of Viral Deception to Guide Industry & Regulatory Responses. *Transatlantic Working Group*. Philadelphia, USA ; Amsterdam, the Kingdom of the Netherlands. 2019. 12 p.

REFERENCES:

1. Denmark warns of Russian spies posing as "journalists or business people". May 5, 2023. URL: https://therecord.media/denmark-russian-spies-warning-journalists-business-people

2. Vilnius Summit Communiqué issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Vilnius 11 July 2023. URL: NATO – Official text: Vilnius Summit Communiqué issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Vilnius 11 July 2023.

3. Bondar, V.T. (2023). Suchasni vyklyky v yevropeiskomu bezpekovomu seredovyshchi: vplyv na systemu natsionalnoi bezpeky Ukrainy. Zb. mater. Mizhnar. nauk.-prakt. konf. "Natsionalna bezpeka Ukrainy v umovakh suchasnykh vyklykiv" (m. Chernihiv, 22 serpnia 2023 roku). Chernihiv: HO "Naukovo-osvitnii innovatsiinyi tsentr suspilnykh transformatsii", 7–10. DOI: https://doi.org/10.54929/conf_22_08_2023-01-01 [in Ukrainian].

4. Multinationals in China accelerate push to decouple data. July 16, 2023. URL: https://archive.ph/df4Wr

5. The Digital Personal Data Protection Bill (2023). *Ministry of Electronics and Information Technology.* New Delhi, India. URL: https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023

6. Svitova hibrydna viina: ukrainskyi front (2017). Monohr. In V.P. Horbulina (Ed.). Kyiv: NISD, 496 p. [in Ukrainian].

7. Trebin, M.P. (2014). "Hibrydna" viina yak nova ukrainska realnist. *Ukrainskyi sotsium*, *3*(50), 113–127 [in Ukrainian].

8. Herasina, L.M., Pohribna, V.L., Polishchuk, I.O. et al. (2015). Politolohichnyi entsyklopedychnyi slovnyk. In M.P. Trebina (Ed.). Kharkiv: Pravo, 816 p. [in Ukrainian].

9. François, C. (2019). Actors, Behaviors, Content: A Disinformation ABC. Highlighting Three Vectors of Viral Deception to Guide Industry & Regulatory Responses. *Transatlantic Working Group*. Philadelphia, USA; Amsterdam, the Kingdom of the Netherlands.