ФІЛОСОФІЯ ТА ПОЛІТОЛОГІЯ В КОНТЕКСТІ СУЧАСНОЇ КУЛЬТУРИ
ISSN 2663-0265 (print) ISSN 2663-0273 (online)
Journal home page: https://fip.dp.ua/index.php/FIP

МІЖНАРОДНІ ВІДНОСИНИ

Олександра Володимирівна ФУРСАЙ
Аспірант Навчально-наукового інституту міжнародних відносин,
Київський національний університет імені Тараса Шевченка,
вул. Володимирська, 60, Київ, 01601, Україна

Oleksandra FURSAI
PhD student,
Educational and Scientific Institute of International Relations,
Taras Shevchenko National University of Kyiv,
St. Volodymyrska, 60, Kyiv, 01601, Ukraine

E-mail: fursai.Al@gmail.com, ORCID: https://orcid.org/0000-0003-1318-4550

УДК 327.88

РОСІЙСЬКА ДЕЗІНФОРМАЦІЙНА КАМПАНІЯ «DOPPELGÄNGER» ЯК НОВІТНІЙ ВИКЛИК ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВ ЗАХОДУ

Received 03 February 2024; revised 19 February 2024; accepted 20 February 2024
DOI: 10.15421/352411

Анотація

Мета. *Метою статті є аналіз російської дезінформаційної кампанії «Doppelgänger», зокрема її сутності, змісту та тактик, як новітньої технологічно складної операції проти колективного Заходу, ціллю якої є дискредитація України в очах світової громадськості та дестабілізація соціально-політичної ситуації в світі.*

Результати. *Дезінформаційна кампанія «Doppelgänger» є новітньою, адаптованою до сучасних інформаційно-технологічних, політичних реалій інформаційною операцією Росії проти Заходу. Використовуючи легку доступність соціальних мереж та їх можливості зі швидкого поширення інформації, Кремль вкотре намагається «викривити» реальність для споживачів інформації на Заході, таким чином створивши сприятливі умови для досягнення своїх зовнішньополітичних цілей.*

Складність цієї конкретної операції в частині протидії їй полягає в технологічній удосконаленості тактик, якими Москва поширює свої наративи. Комбіноване використання штучного інтелекту, методу клонування сайтів, створення мережі «маріонеток» в соцмережах створює нові виклики для інформаційної безпеки колективного Заходу, існуючі відповіді на які наразі не є достатніми для нівелювання загрози. Як наслідок, актуальною та нагальною є швидка адаптація до нових викликів та розробка засобів протидії їх негативному впливу.

Наукова новизна. *Наразі кампанія «Doppelgänger» є недостатньо досліджена науковою спільнотою, як в Україні, так і за кордоном, а наявні сьогодні розвідки у цьому напрямку обмежуються висвітленням виключно практичної складової кампанії, без прив'язки до теоретичних праць з дослідження інформаційного впливу в сучасній системі міжнародних відносин.*

Практична цінність. *Результати статті можуть бути використані науковцями для поглиблення дослідження стратегії гібридної війни Росії проти Заходу, зокрема її інформаційної компоненти. Також вони можуть бути використані урядовими структурами держав Заходу, зокрема України, при плануванні та розбудові системи реагування та протидії «Doppelgänger» та іншим подібним дезінформаційним кампаніям Росії.*

Ключові слова: війна, кібербезпека, пропаганда, «м'яка сила», гібридна війна, інформаційна безпека, «гостра сила», інформаційна політика, «штучний інтелект», інформаційна війна, дезінформація, санкції Росія, Україна, ЄС, Німеччина, НАТО, RT.

THE RUSSIAN DISINFORMATION CAMPAIGN «DOPPELGÄNGER» AS THE NEWEST CHALLENGE TO THE INFORMATION SECURITY OF WESTERN STATES

Abstract

Purpose*. The purpose of the article is to analyse the Russian disinformation campaign "Doppelgänger", in particular its essence, content and tactics, as the latest technologically complex operation against the collective West, the goal of which is to discredit Ukraine in the eyes of the world public and destabilise the socio-political situation in the world.*

Results. *The "Doppelgänger" disinformation campaign is Russia's latest information operation against*

the West, adapted to modern information technology and political realities. Using the easy availability of social networks and their ability to quickly spread information, the Kremlin is once again trying to "distort" reality for information consumers in the West, thus creating favourable conditions for achieving its foreign policy goals.

The complexity of this particular operation in terms of countering it lies in the technological sophistication of the tactics by which Moscow spreads its narratives. The combined use of artificial intelligence, the method of cloning sites, and the creation of a network of "puppets" in social networks creates new challenges for the information security of the collective West, the existing answers to which are currently insufficient to level the threat. As a result, rapid adaptation to new challenges and the development of means of counteracting their negative impact are urgent and urgent.

***Scientific novelty.** Currently, the "Doppelgänger" campaign is insufficiently researched by the scientific community, both in Ukraine and abroad, and today's intelligence in this direction is limited to coverage of the exclusively practical component of the campaign, without reference to theoretical works on the study of information influence in the modern system of international relations.*

***Practical value.** Scientists can use the results of the article to deepen the study of Russia's hybrid war strategy against the West, in particular its informational component. They can also be used by government structures of Western countries, in particular Ukraine when planning and building a system for responding to and countering "Doppelgänger" and other similar Russian disinformation campaigns.*

Key words: war, cybersecurity, propaganda, "soft power", hybrid war, information security, "sharp power", information policy, artificial intelligence, information war, disinformation, sanctions, Russia, Ukraine, EU, Germany, NATO, RT.

Постановка проблеми.

Однією з характерних ознак сучасного стану системи міжнародних відносин є зростання ролі інформації як фактору геополітичної потужності держави на міжнародній арені. Це змушує провідні держави світу приділяти все більшу увагу нарощуванню власних «інформаційних м'язів». Якщо в демократіях це полягає у покращенні власної інформаційної безпеки, тобто «обороні», то авторитарні та тоталітарні режими використовують ці «м'язи» для «наступу», зокрема тиску на власне населення та на інші держави. Одним із «лідерів» у цьому є Росія, яка активно використовує дезінформацію для досягнення своїх внутрішньо- та зовнішньополітичних цілей, зокрема у протистоянні з колективним Заходом. Найновіша російська дезінформаційна кампанія «Doppelgänger» представляє собою новий виклик європейській інформаційній безпеці та інформаційним політикам держав Заходу. Ця кампанія, спрямована на дискредитацію України в очах громадськості Заходу та дестабілізацію соціально-політичної ситуації в державах Європи, використовує новітні інформаційні та технологічні підходи, тактики для маніпулювання громадською думкою та впливу на систему прийняття рішень в європейських державах. Серед таких тактик, які дозволяють створити індивідуалізовані підходи для впливу на різні аудиторії, – розповсюдження фейків в соцмережах, використання штучного інтелекту та маніпулювання децентралізованим характером інтернету для генерування «клонів» визнаних медіа. Це створює серйозні виклики для систем інформаційної безпеки в Європі та вимагає розробки та впровадження нових стратегій та технологій для протидії таким кампаніям. Окрім того, міжнародне співробітництво у сфері інформаційної безпеки стає важливою складовою для протистояння цьому новому виклику та забезпечення стабільності в інформаційному просторі.

Аналіз попередніх досліджень та публікацій. Основою для вивчення даної теми стали дослідження Європейської неурядової організація EU DisinfoLab, що стоїть біля витоків дезінформаційної операції «Doppelgänger», а також дослідження Insikt Group, що було проведено у 2023 році.

Мета дослідження. Дослідити ключові методи, прийоми та засоби дезінформаційної кампанії «Doppelgänger» проти країн колективного Заходу, зокрема України.

Методи та прийоми дослідження.

Дослідження дезінформаційної кампанії

«Doppelgänger» вимагає використання різних методів та прийомів, оскільки це складний процес, пов'язаний з розкриттям та аналізом великого обсягу інформації. У цій статті було використано системно-історичний метод. Цей метод дослідження є важливим інструментом для вивчення проблеми та її складових в контексті конкретної історичної ситуації. Цей метод дозволяє аналізувати взаємозв'язану систему явищ та подій відносно певного періоду часу, враховуючи вплив зовнішніх факторів на розвиток суспільства. В конкретному випадку дослідження впливу ворожої держави на європейське суспільство.

Виклад основного матеріалу.

Держави та політичні лідери завжди прагнуть роз'яснювати свої позиції та рішення так, щоб продемонструвати себе у вигідному світлі. Це є абсолютно нормальним явищем, адже у демократії політичні лідери зобов'язані доносити до населення свої цілі та цінності. Однак деякі суб'єкти заходять набагато далі правомірної «публічної дипломатії», подаючи свої методи вирішення світових проблем як єдино ефективні та намагаючись дискредитувати решту. Деякі іноземні суб'єкти – як державні, так і недержавні – навіть ведуть кампанії з дезінформації, навмисно розповсюджуючи відомості, які вводять в оману, щоб послабити те чи інше суспільство і підірвати його здатність ефективно реагувати на кризи. Завдяки можливостям інтернету дезінформація поширюється швидше, ніж раніше, доходячи до кожного будинку в режимі нон-стоп. Деякі держави, наприклад Росія і Китай, активно займаються цією діяльністю, намагаючись підірвати і повалити демократичні системи, а також поставити під сумнів цінності свободи, плюралізму, стримувань і противаг, що лежать в основі європейського суспільства та, загалом, суспільства Заходу.

Суперечки про те, як досягти влади – використанням танків чи ідеями – також не є новою. Ті, хто вбачає владу як результат стримування, дотримуються теорії «жорсткої сили» [Gray 2011]. Ця теорія відбиває погляд на міжнародні відносини школи політичного реалізму, створеної Гансом Моргентау. Так держави нав'язують свою волю у вигляді військової сили чи економічного впливу [Political Realism 2023].

Однак, у 1990 році професору Гарвардського інституту державного управління імені Джона Кеннеді та майбутньому раднику Білла Клінтона Джозефу Наю спала на думку ідея «м'якої сили» [Nye 2004]. Як пояснює Джозеф Най, «м'яка сила» означає змусити решту силою переконання робити те, що хочеш ти. Фактично «м'яка сила» означає, що держава може використовувати свою соціальну привабливість, власну культуру, свої цінності за її межами, якщо ця країна сама ж слідує їм у своїй внутрішній політиці. І якщо країна робить це законно, то і її зовнішня політика може виявитися привабливою [Nye 2003].

Так і було довгий час, поки всього кілька років назад світ не зіткнувся з новим явищем, яке дослідники характеризують як «гостру силу». Концепція «гострої сили», суть якої полягає у досягненні геополітичних інтересів шляхом використання маніпуляцій, дезінформації, точкових інформаційних операцій, була запропонована американськими дослідниками К.Волкером та Д.Людвігом. Дана концепція набуває все більшої значущості протягом останніх років. Так, яскравим прикладом реалізації даної концепції є сьогоднішня політика Китаю та Росії [Walker, Kalathil & Ludwig 2018].

Якщо ми говоримо про російський зовнішньополітичний вплив, то виникає дилема. Річ у тім, що Росія використовує такі ж самі інструменти, які використовують й інші демократичні країни, коли намагаються проводити політику «м'якої сили». До таких інструментів ми відносимо публічну дипломатію, культурні заходи, роботу з лідерами громадської думки певних країн, студентські обміни тощо. Саме тому те, що світ досі розумів під «м'якою силою», у випадку з російською пропагандою краще класифікувати як «гостру силу», яка «пронизує» та «вторгається» в політичне та інформаційне середовище країн-мішеней. І якщо у випадку з «м'якою силою» від її застосування виграють обидві сторони, то застосування «гострої сили» це завжди гра з «нульовою сумою». Країна-мішень в результаті застосування «гострої сили» Кремля нічого

хорошого не отримує [Walker & Ludwig 2021] [Walker 2018].

Дослідження поняття «гострої сили» проводяться у різних напрямках. В одних працях «гостра сила» розглядається як форма влади «авторитарних режимів» (насамперед Росії, Китаю та Ірану) [Yenna 2019: 129-153] [Walker & Ludwig 2017].

Друга група досліджень присвячена методології вивчення «гострої сили» як нового феномену міжнародних відносин [Hanouna, Neu, Pardo, Tsur & Zahavi 2019: 97-113].

Деякі дослідники задаються питанням про правомірність виділення «гострої сили» в окрему концепцію. Зазначається, що «гостра сила» може бути ідеологічною маніпуляцією та «пропагандистським кліше» [Shao 2019: 129-148].

На думку одного з дослідників Гарвардського університету та стипендіата програми Фулбрайта в університеті Джорджа Вашингтона Франсіско Родрігес-Хіменеса, поняття «гостра сила» прийшло на зміну терміну «пропаганда». За його словами, пропаганда спрямована на швидке досягнення результату, в той час як «гостра сила» потребує більш тривалого часу для впливу на громадську думку, як і «м'яка сила» [Poder afilado: 2018]. Чи можемо ми в такому випадку твердити, що російська пропаганда маскується під «м'яку силу» – покаже час.

Сучасна інформаційна війна стала частиною нашого повсякдення, яку Росія веде вже багато десятків років. Російська Федерація використовує різні медійні платформи, включаючи онлайн-видання та телебачення, для проведення інформаційної війни проти України, активно поширюючи пропаганду, яка зазвичай відображає несправжню картину подій. Після повномасштабного вторгнення Росії на територію України у 2022 році набирає обертів і повномасштабна гібридна війна. в різних напрямках, оскільки це не обмежується лише інформаційною війною. Вона також включає в себе економічні, політичні, а також військові аспекти, що охоплюють боротьбу за ідеології та світогляди. Це комплексна стратегія, що впливає на різні сфери суспільства та визначається різноманітністю своїх напрямків, таких як економіка, політика, інформаційна сфера та культурне сприйняття [Сабрі 2018].

Враховуючи цю ситуацію, одним із ключових завдань для світу стає вміння виявляти інформаційний вплив, інформаційно-психологічні операції (ІПСО) та встояти перед ними. Це передбачає розуміння причин та методів, які використовуються на сучасному «інформаційному фронті».

Концепція «гібридної війни», яку розробив Френк Хоффман, консультант міністерства ВМФ США, визначає, що в кожній епосі існують унікальні форми війни. За його словами, у сучасній епосі спостерігається процес гібридизації, який також впливає на військову сферу. Традиційні форми війни поєднуються з організованою злочинністю, тероризмом та іррегулярними конфліктами. Ця концепція відображає змінену природу сучасних конфліктів, де різні методи та стратегії використовуються разом для досягнення воєнно-політичних цілей [Hoffman 2009: 34-39]. Запропоноване поняття «гібридна війна» використовується для опису та характеризації сучасного феномену, що відображає сутність змін у природі війни. Цей термін оперативно віддзеркалює еволюцію предметності сучасних конфліктів та вказує на виникнення нового типу воєнних ситуацій – гібридних, інформаційних [Магда 2015].

Саме інформаційна складова, яка була активізована ще до повномасштабного вторгнення і взаємодіяла зі збройною агресією у подальшому, є одним із ключових аспектів у гібридній війні Росії проти України. Інформаційна кампанія адаптується до поточних завдань і спрямована на громадян усіх регіонів України, Росії та країн Європи. Вона має різні цільові установки, які реалізуються через вплив на ментально-психологічний стан та суспільну свідомість.

Основною метою інформаційної війни РФ в Україні є знищення державності, в Росії – виправдання рішень російського керівництва для отримання підтримки своїх громадян, а в Європі – дискредитація України як держави, уряду, Збройних Сил, а також, в широкому розумінні, дискредитація НАТО, ЄС та європейських цінностей. Таким чином, інформаційна

війна стає викликом не тільки для України та всієї міжнародної спільноти, а також загрозою світовому порядку.

Так, у лютому 2022 року Кремль запустив чергову потужну інформаційну операцію проти України та держав колективного Заходу. Головна мета цієї операції полягає в підриві підтримки України у відбитті агресії Росії шляхом «демонізації» українського уряду в очах світової спільноти та звинувачення його у «нацизмі» та корупції. Також вона ставить за мету посіяти розбіжності в державах, які підтримують Україну, стверджуючи, що фінансова підтримка України та впровадження санкцій проти Росії в кінцевому підсумку призводять до невдачі [Doppelganger operation 2024]. Ця кампанія отримала назву «Doppelgänger» (від нім. – «двійник») через систематичне використання підроблених клонів офіційних веб-сайтів як медіа-організацій, так і державних установ. Також ця кампанія, організаторами якої є дві російські компанії Struktura та Social Design Agency (також відомі як ASP), відома під назвою RRN (Recent Reliable News) [RRN 2023].

Основними країнами, які стали об'єктом цієї інформаційної операції, стали Франція, Німеччина, Україна, Латвія, Італія, Велика Британія, США та Польща. Особливо варто відмітити Францію та Німеччину, які стали ключовими мішенями в цій операції [Doppelganger operation 2024].

Так, в червні 2023 року французький уряд виявив ворожу інформаційну кампанію, що була спрямована проти Франції, і в якій були задіяні російські суб'єкти. Зокрема, у цій кампанії, в основі якої було поширення неправдивої інформації, брали участь державні чи пов'язані з російською державою організації. Так, ця кампанія ґрунтується на створенні неправдивих веб-сторінок, що імітують сайти національних ЗМІ та урядових органів, а також на створенні фейкових облікових записів у соціальних мережах. Тактика включала використання «typosquatting» (метод, який передбачає реєстрацію домену зі свідомими друкарськими помилками з ціллю імітації назв популярних сайті) для реєстрації доменних імен на альтернативних реєстраторах DNS. Це дозволяло їм видавати себе за автентичні джерела інформації. Зміст фокусувався на публікації фейкових урядових заходів та подій.

Французькій службі VIGINUM вдалося завчасно виявити цю кампанію, що дозволило компетентним французьким органам вжити захисних та превентивних заходів. Наразі проводяться інші належні технічні заходи. Зокрема, Міністерство Європи та закордонних справ вчасно запобігло спробі імітації свого сайту [Déclaration de Catherine Colonna 2023].

Проведені розслідування VIGINUM дозволили виявити численні докази, що вказують на причетність російських чи російськомовних осіб та низки російських компаній до реалізації та проведення цієї кампанії. У VIGINUM також зазначили, що низка державних чи пов'язаних із російською державою організацій брали участь у поширенні деяких матеріалів, створених у рамках зазначеної кампанії. Залучення російських посольств та культурних центрів, які взяли активну участь у розширенні масштабів цієї кампанії, зокрема через свої офіційні акаунти в соціальних мережах, є черговим свідченням гібридної стратегії, яку реалізує Росія з метою дестабілізувати роботу демократичних інститутів Заходу [Déclaration de Catherine Colonna 2023] [Media Clones 2022].

Загалом, «Doppelgänger» включає низку тактик для успішної реалізації своєї операції. Серед таких варто відмітити клонування урядових сторінок та сторінок відомих медіа-сайтів, таких як Le Monde, The Guardian, Ansa, Der Spiegel і Fox News. Ці клони намагалися імітувати офіційні сайти видань, розміщуючи фейкові новини та інформацію. Для створення таких клонів спеціально використовувалися помилки в доменних іменах, наприклад, використання альтернативних реєстраторів DNS та тематичних розширень, таких як .ltd, .online чи .foo. Це робило клони менш помітними та складнішими для виявлення [Avdeenko 2023]. Так, було створено клони офіційних сторінок Міністерства Європи та закордонних справ Франції, Міністерства внутрішніх справ Німеччини та Північноатлантичного альянсу (НАТО) [Antoniuk 2023].

Іншою тактикою є створення антиукраїн-

ських веб-сайтів, що постійно наповнювалися антиукраїнським контентом спрямованим проти Президента України Володимира Зеленського. Цей контент використовував анімаційні фільми та карикатури для створення негативного враження про українського лідера та уряду України. Аналогічно було створено низку проросійських веб-сайтів таких як «War On Fakes» та «RRN». Ці сайти поширювали пропаганду та атакували Захід, представляючи себе як надійні джерела інформації [Doppelganger operation 2024].

На початку листопада 2023 року «зірки Давида», які можуть трактуватися як символ «проти» чи «за» Ізраїль, з'явилися на будівлях у Парижі. Зображення цих зірок швидко розповсюдилося в соціальних мережах, спричиняючи суперечки та плутанину. Державна технічна та оперативна служба Франції, яка відповідає за захист від зовнішніх цифрових перешкод, VIGINUM виявила, що мережа, що стояла за цим явищем, включала понад тисячу ботів на платформі X (раніше – Twitter), які були афілійовані з RRN [Nouvelle ingérence numérique 2023]. Це може трактуватися як елемент потенційної гібридної операції, оскільки вона не лише викликає непорозуміння, а й може впливати на громадську думку та викликати соціальні конфлікти. Враховуючи зв'язок цього явища із RRN, можна припустити, що це є частиною стратегії впливу та дезінформації, спрямованої на досягнення певних політичних чи геополітичних цілей, які переслідує Росія.

В основному для поширення свого контенту та реклами «Doppelgänger» використовувала соцмережі Facebook, X, Dailymotion та Instagram. Іноді вони інвестували кошти в рекламу на платформах, щоб забезпечити більше охоплення. Ці тактики дозволяли «Doppelgänger» ефективно маскувати свою діяльність та впливати на громадську думку в країнах-мішенях [Doppelganger operation 2024].

Згідно дослідження, що було проведене Insikt Group у 2023 році, тактики «Doppelgänger» демонструють високий рівень витонченості, включаючи передові методи обфускації та, ймовірно, використання генеративного штучного інтелекту (ШІ) для створення оманливих новинних статей. Здібності «Doppelgänger» до адаптації є прикладом стійкого характеру російської інформаційної війни зі стратегічним фокусом на поступовій зміні громадської думки та поведінки. Використання генеративного ШІ для створення контенту означає еволюцію в тактиці, що відображає ширшу тенденцію використання ШІ в кампаніях інформаційної війни. У міру зростання популярності генеративного штучного інтелекту зловмисники, такі як ті, що стоять за «Doppelgänger», все частіше будуть використовувати ШІ для масштабування свого впливу [Obfuscation AI Content 2023].

Інцидент, що стався у листопада 2023 року, свідчить про продовження російських дезінформаційних кампаній, спрямованих на дискредитацію Президента України Володимира Зеленського. Публікація відео на рекламному щиті на одній з найлюдяніших вулиць Нью-Йорку – Тайм-сквер, з репером і актором Снуп Доггом є цікавим прикладом обґрунтованої дезінформації з використанням deep fake та ШІ [Russian Disinformation 2024]. У цьому випадку використання видатної особи, такої як Снуп Догг, для подачі фейкового повідомлення про «наркотичні звички» Володимира Зеленського має на меті не лише розповсюдження неправдивої інформації, але й залучення уваги громадськості з допомогою популярного артиста. Фактично ця кампанія використовує особистість Снуп Догга щодо припинення вживання наркотиків, щоб штучно створити зв'язок з В. Зеленським, підкреслити його вигадану «наркозалежність» та вплинути на громадську думку. Це ще один приклад того, як дезінформація може використовувати сучасні засоби комунікації для досягнення своїх цілей, використовуючи різноманітні соціальні мережі та рекламні платформи.

Відео стало частиною нової кампанії в X (раніше Twitter), яка використовує техніку, визначену AFP як «Матрьошка». У кампанії використовуються два різних рівня «маріонеток». Перший рівень «маріонеток» відповідає за публікацію підробленого вмісту, а друга група облікових записів відповідає за цитування

матеріалу з посиланням на ЗМІ та фактчекінгові платформи. Мета цього підходу проста і спрямована на подовження терміну існування облікових записів, які поширюють фейковий вміст (другий рівень), оскільки облікові записи, які є джерелом дезінформації, часто швидко призупиняються (перший рівень). У той час як кампанія «Doppelgänger» націлена на широку громадськість, то у колаборації з «Матрьошка» вони разом націлюються на ЗМІ та фактчекерів, успішно перевантажуючи їх фальшивими запитами перевірки фактів [Matriochka la nouvelle campagne 2024].

Дезінформаційна кампанія «Doppelgänger» та техніка «Матрьошка» є відзеркаленням адаптації Росії до сучасних реалій, де традиційні засоби впливу на Заході, зокрема через традиційні ЗМІ, стали менш ефективними. Адже після санкцій ЄС, які були введені щодо російських пропагандистських ресурсів Sputnik і Russia Today (RT) та інших пропагандистських ЗМІ, Росії стало важче реалізовувати дезінформаційні кампанії [EU sanctions 2023].

Як ми бачимо, російська влада виявила високий рівень гнучкості та стратегічного мислення, шукаючи нові шляхи впливу на громадську думку та формування світогляду. Одним із ключових компонентів цієї адаптації стала активна експлуатація інтернет-простору, включаючи соціальні мережі та онлайн-медіа. «Doppelgänger» використовує різноманітні техніки, такі як підробка новин, маніпуляція соціальними мережами та імітація авторитетних джерел, щоб впливати на громадську думку та створювати враження широкої підтримки або обурення. Ця стратегія дозволяє Росії обходити традиційні механізми контролю та протидії, оскільки інтернет надає можливість розповсюдження інформації швидко та у великих обсягах. Адаптація до нових реалій включає в себе і використання технологій ШІ для створення обманливого контенту та оптимізації стратегій впливу. Таким чином, «Doppelgänger» стає елементом нового підходу Росії до інформаційної війни, орієнтованого на використання сучасних інтернет-ресурсів для досягнення своїх політичних та геополітичних цілей.

Захід реагує на цей новий виклик традиційним накладенням санкцій на організаторів. Рішення Ради Європейського Союзу ввести обмежувальні заходи проти осіб та організацій, відповідальних за кампанію маніпулювання цифровою інформацією під назвою «RRN» (Recent Reliable News), свідчить про серйозність загрози, яку представляє дезінформація для інформаційної безпеки та стабільності регіону [Information manipulation 2023].

Обмежувальні заходи можуть включати різні санкції проти фізичних осіб та організацій, такі як заморожування активів, заборона в'їзду та інші економічні обмеження. Такі заходи призначені для покарання та стримування тих, хто відповідає за дезінформаційні кампанії, і мають за мету запобігти подібним акціям у майбутньому. Це також може бути частиною більш широкої стратегії ЄС у сфері кібербезпеки та захисту від гібридних загроз. Важливою складовою таких заходів є співпраця між країнами ЄС, обмін інформацією та розробка спільних стратегій для боротьби з дезінформацією та кіберзагрозами. Не дивлячись на зусилля з боку країн ЄС, результат все ще слабкий і значна частина фейкових акаунтів продовжує діяти. Висновки підкреслюють важливість постійної співпраці та публічного звітування між державами для підвищення обізнаності та підвищення онлайн-грамотності у протидії зловмисному впливу. Медіа-організації, зокрема, заохочуються проактивно відстежувати ворожу активність під час таких операцій і оперативно реагувати. Незважаючи на розголошення діяльності «Doppelgänger», його постійна еволюція та використання ШІ свідчать про потенційні довгострокові наслідки для суспільства, включаючи ерозію громадської довіри та посилення поляризації.

Дослідження дезінформаційної кампанії «Doppelgänger» та обмежувальних заходів, вжитих Заходом, мають надзвичайну актуальність для України, яка знаходиться в епіцентрі гібридної війни Росії проти колективного Заходу. У контексті дослідження «Doppelgänger» та інших подібних кампаній можна виділити спроби впливу на громадську думку, дестабілізацію суспільства та створення хаосу через розповсюдження дезінформації та фейкових

інформаційних ресурсів на території України. Прикладом може служити кейс пов'язаний з впливовим медіа-ресурсом «РБК Україна». У вересні 2023 року було виявлено створення «клону» офіційної сторінки медіа, який імітував зовнішній вигляд офіційної сторінки та просував прокремлівські наративи [Україна продає 2023]. Кейс з РБК Україна є яскравим прикладом того, як російські дезінформаційні кампанії спрямовані на знищення довіри до незалежних ЗМІ та розмивання меж між об'єктивними новинами та маніпулюванням інформацією [Фейкове опитування 2022].

Підкреслимо, що в умовах сучасних гібридних викликів, які створює РФ, ефективна протидія держав Заходу, зокрема України, подібним дезінформаційним кампаніям повинна передбачати не тільки заходи із захисту власного інформаційного простору, але й скоординовані контрнаступальні дії, спрямовані на російський інформаційний простір. Тобто, йдеться про застосування так званої стратегії «активної оборони», коли жертва систематичних інформаційних атак не тільки реагує, але й сама створює виклики для інформаційної безпеки агресора.

У цьому контексті важливо наголосити, що попри жорсткий контроль Кремлем власного інфопростору, зокрема таких соцмереж як «ВКонтакте», «Одноклассники», а також блокування глобальних соціальних майданчиків Facebook та X, все ще чутливими для потенційних контрнаступальних дій Заходу є такі соцмережі як YouTube та Telegram, які користуються значною популярністю в Росії.

Проте, слід зауважити, що будь-які скоординовані дії Заходу з протидії дезінформаційним кампаніям Кремля шляхом створення інформаційних контраргументів повинні ґрунтуватися на принципі використання правди як ключового опонента російській дезінформації. Тобто, йдеться про створення «стратегії інформування» як противаги «стратегії дезінформування».

Бібліографічні посилання / References

Магда, Є. (2015). *Гібридна війна: вижити і перемогти.* Х.: Vivat. / Mahda, Ye. (2015). *Hibrydna viina: vyzhyty i peremohty.* Kh.: Vivat. (in Ukrainian)

Зловмисники проводять фейкове опитування від імені «РБК-Україна». (2022). *Детектор медіа.* / Zlovmysnyky provodiat feikove opytuvannia vid imeni «RBK-Ukraina». (2022). *Detektor media.* Retrieved January 15, 2024 from https://detector.media/infospace/article/200895/2022-07-11-zlovmysnyky-provodyat-feykove-opytuvannya-vid-imeni-rbk-ukraina/ (in Ukrainian)

Сабрі. (2018). Інформаційно-іміджевий аспект гібридної війни. *Молодий вчений*, (5), 206-210. / Sabri. (2018). Informatsiino-imidzhevyi aspekt hibrydnoi viiny. *Molodyi vchenyi,* (5), 206-210. (in Ukrainian)

«Україна продає дітей на нелегальних ринках» і «ухилянти ховаються у вишах»: росіяни створюють клони українських новинних медіа. (2023). *SPRAVDI*. / «Ukraina prodaie ditei na nelehalnykh rynkakh» i «ukhylianty khovaiutsia u vyshakh»: rosiiany stvoriuiut klony ukrainskykh novynnykh media. (2023). *SPRAVDI.* Retrieved January 15, 2024 from https://spravdi.gov.ua/ukrayina-prodaye-ditej-na-nelegalnyh-rynkah-i-uhylyanty-hovayutsya-u-vyshah-rosiyany-stvoryuyut-klony-ukrayinskyh-novynnyh-media/ (in Ukrainian)

Antoniuk, D. (2023). Russia-linked "Doppelgänger" social media operation rolls on, report says. *The Record.* Retrieved January 16, 2024 from https://therecord.media/doppelganger-influence-operation-new-activity

Déclaration de Catherine Colonna - Ingérences numériques étrangères – Détection par la France d'une campagne de manipulation de l'information. (2023). *France Diplomatie.* Retrieved January 14, 2024 from https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/actualites-et-evenements-lies-a-la-securite-au-desarmement-et-a-la-non/2023/article/declaration-de-catherine-colonna-ingerences-numeriques-etrangeres-detection-par

Doppelganger Media clones serving Russian propaganda. (2022). *EU Disinfo Lab.* Retrieved January 18, 2024 from https://www.disinfo.eu/wp-content/uploads/2022/09/Doppelganger-1.pdf

Doppelganger operation. (2024). *EU Disinfo Lab.* Retrieved February 2, 2024 from https://www.disinfo.eu/doppelganger-operation/

EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU. (2022). *European Commission.* Retrieved January 21, 2024 from https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rt-russia-today-and-sputnik-s-broadcasting-in-the-eu/

Gray, C. (2011). HARD POWER AND SOFT POWER: THE UTILITY OF MILITARY FORCE AS AN INSTRUMENT OF POLICY IN THE 21ST CENTURY. *Strategic Studies Institute.* Retrieved January 11, 2024 from https://www.files.ethz.ch/isn/128690/pub1059-1.pdf

Hanouna, Pardo, Neu, Tsur & Zahavi. (2019). Sharp Power in Social Media: Patterns from Datasets across Electoral Campaigns. *Australian and New Zealand Journal of European Studies,* 11(3), 97-113.

Hoffman, F. (2009). Hybrid Warfare and Challenges. *Joint Force Quarterly (JFQ)*, (52), 34-39.

Information manipulation in Russia's war of aggression against Ukraine: EU lists seven individuals and five entities. (2023). *European Council*. Retrieved January 15, 2024 from https://www.consilium.europa.eu/en/press/press-releases/2023/07/28/information-manipulation-in-russia-s-war-of-aggression-against-ukraine-eu-lists-seven-individuals-and-five-entities/

«Matriochka», la nouvelle campagne de désinformation anti-ukrainienne à destination des médias occidentaux. (2024). *AFP Factuel.* Retrieved January 30, 2024 from https://factuel.afp.com/doc.afp.com.34H32VP

Nye, J. (2005). *Soft Power. The Means to Success in World Politics. Public Affairs.*

Obfuscation and AI Content in the Russian Influence Network "Doppelgänger" Signals Evolving Tactics. (2023). *Recorded Future.* Retrieved January 22, 2024 from https://go.recordedfuture.com/hubfs/reports/ta-2023-1205.pdf

Poder afilado: cómo China y Rusia quieren conquistar el mundo. (2018). *El Mundo.* Retrieved January 10, 2024 from https://www.elmundo.es/papel/historias/2018/03/03/5a993938e5fdeaac5b8b4586.html.

Political Realism in International Relations. (2023). *Stanford Encyclopedia of Philosophy*. Retrieved January 15, 2024 from https://plato.stanford.edu/entries/realism-intl-relations/#HansMorgRealPrin

RRN: A complex and persistent information manipulation campaign. (2023). *Secretariat general de la defense et de securite nationale.* Retrieved January 19, 2024 from https://www.sgdsn.gouv.fr/files/files/20230719_NP_VIGINUM_RAPPORT-CAMPAGNE-RRN_EN1.pdf.

RUSSIAN DISINFORMATION AGAINST ZELENSKYY EXPOSED ON TIMES SQUARE BILLBOARD. (2024). *Qurium media foundation.* Retrieved February 2, 2024 from https://www.qurium.org/alerts/russian-disinformation-against-zelenskyy-exposed-on-times-square-billboard/

Russie – Nouvelle ingérence numérique russe contre la France. (2023). *France Diplomatie.* Retrieved January 20, 2024 from https://www.diplomatie.gouv.fr/fr/dossiers-pays/russie/evenements/evenements-de-l-annee-2023/article/russie-nouvelle-ingerence-numerique-russe-contre-la-france-09-11-23

Shao, J. (2019). Exploring China's "Sharp Power": Conceptual Deficiencies and Alternatives. Transcommunication, 6-2, 129-148.

Walker C. (2018). What Is Sharp Power? *Journal of Democracy,* 29, 9-23.

Walker C. (2017). The Meaning of Sharp Power. How Authoritarian States Project Influence. *Foreign Affairs.* Retrieved January 13, 2024 from https://www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power

Walker C. (2021). *The Long Arm of the Strongman. How China and Russia Use Sharp Power to Threaten Democracies Foreign Affairs.* Retrieved January 15, 2024 from https://www.foreignaffairs.com/china/long-arm-strongman

Walker, C., Kalathil, S., & Ludwig, J. (2018). Forget Hearts and Minds. *Foreign Policy.* Retrieved January 23, 2024 from https://foreignpolicy.com/2018/09/14/forget-hearts-and-minds-sharp-power/

Yenna W. (2019). Recognizing and Resisting China's Evolving Sharp Power. *American Journal of Chinese Studies*, 26, 129-153.