УДК (UDC) 32.019.51
DOI: 10.26693/ahpsxxi2023.si.093

THE USE OF SOCIAL MEDIA AS A TOOL OF MODERN HYBRID WARFARE

Olena Kuchmii,
e-mail: kuchmiy.olena@gmail.com
ORCID: https://orcid.org/0000-0002-2634-4114
Educational and Scientific Institute of International Relations,
Taras Shevchenko National University of Kyiv,
Ukraine, 04119, Kyiv, Yuriia Illienka St, 36/1

Oksana Frolova,
e-mail: sancha279@ukr.net
ORCID: https://orcid.org/0000-0001-7105-2762
Educational and Scientific Institute of International Relations
Taras Shevchenko National University of Kyiv,
Ukraine, 04119, Kyiv, Yuriia Illienka St, 36/1

Abstract

The modern security architecture is formed under the influence of a number of new factors and threats, among which the most dangerous are hybrid wars, an important feature of which is the active use of information methods of confrontation, which involve a situational combination of various means of conducting information warfare, conducting informational and psychological operations, conducting propaganda campaigns, as well as modern technological achievements, in particular, artificial intelligence technologies, to carry out large-scale attacks, which are becoming increasingly difficult to resist. The most dynamic space of confrontation between the actors of international relations today is social media, which open unique opportunities for carrying out large-scale, complex, multidimensional cross-border cybernetic and informational-psychological attacks on states and state institutions, as well as on individuals. The main advantages of using social media include the scale of audience coverage, accessibility, speed of information dissemination, anonymity, the ability to exchange large amounts of data, and the absence of geographical or content restrictions. The purpose of the article is to study the theory and practice of using social media as an effective tool of hybrid warfare in the modern world.

Taking into account the relevance of this topic, the article considers the main characteristics of social media from the standpoint of their use in hybrid wars, analyzes the most common ways, methods and techniques of using social media in hybrid warfare, defines the specifics of the use of "social cyberattacks", "astroturfing", internet trolling. The scientific work also presents an analysis of the use of social networks and messengers in the hybrid war of the Russian Federation against Ukraine on the example of YouTube and Telegram and shows how Russian propaganda media use them to increase the audience and simplify the delivery of manipulative and false information to consumers in Russia itself and in Ukraine and the world.

Keywords: Ukraine, Russian Federation, hybrid war, social media, fakes, disinformation, Internet trolling, YouTube, Telegram

ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕДІА ЯК ІНСТРУМЕНТУ СУЧАСНОЇ ГІБРИДНОЇ ВІЙНИ

Олена Кучмій,
e-mail: kuchmiy.olena@gmail.com
ORCID: https://orcid.org/0000-0002-2634-4114
Навчально-науковий інститут міжнародних відносин
Київського національного університету імені Тараса Шевченка,
Україна, 04119, м. Київ, вул. Юрія Іллєнка, 36/1

Оксана Фролова,
e-mail: sancha279@ukr.net
ORCID: https://orcid.org/0000-0001-7105-2762
Навчально-науковий інститут міжнародних відносин
Київського національного університету імені Тараса Шевченка,
Україна, 04119, м. Київ, вул. Юрія Іллєнка, 36/1

Анотація

Сучасна архітектури безпеки формується під впливом низки нових чинників і загроз, серед яких найбільш небезпечними виступають гібридні війни, важливою рисою яких є активне використання інформаційних методів протиборства, що передбачають ситуативне поєднання різних засобів ведення інформаційної війни, проведення інформаційно-психологічних операцій, здійснення пропагандистських кампаній, а також сучасних технологічних досягнень, зокрема, технологій штучного інтелекту, для здійснення масштабних атак, протистояти яким стає дедалі складніше. Найбільш динамічним простором протистояння акторів міжнародних відносин нині виступають соціальні медіа, що відкривають унікальні можливості для здійснення масштабних, комплексних, багатовимірних транскордонних кібернетичних та інформаційно-психологічних атак як на держави та державні інститути, так й на окремих осіб. До основних переваг використання соціальних медіа відноситься масштабність охоплення аудиторії, доступність, швидкість поширення інформації, анонімність, можливість обміну великими масивами даних, відсутність географічних або змістових обмежень. Метою статті є дослідження теорії і практики використання соціальних медіа як ефективного інструменту гібридної війни у сучасному світі.

Враховуючи актуальність даної теми, у статті розглянуто основні характеристики соціальних медіа з позиції їх використання у гібридних війнах, проаналізовано найбільш поширені способи, методи і прийоми використання соціальних медіа у гібридному протиборстві, визначено специфіку застосування «соціальних кібератак», «астротурфінгу», інтернет-тролінгу. У науковій праці також представлено аналіз використання соціальних мереж і месенджерів у гібридній війни РФ проти України на прикладі YouTube та Telegram та показано, як російські пропагандистські ЗМІ використовують їх для збільшення аудиторії та спрощення донесення маніпулятивної та брехливої інформації до споживачів як у самій Росії, так й в Україні та світі.

Ключові слова: Україна, РФ, гібридна війна, соціальні медіа, фейки, дезінформація, інтернет-тролінг, YouTube, Telegram

Постановка проблеми. Трансформація системи міжнародної безпеки зумовлена потребою вироблення нових ефективних механізмів протидії сучасним викликам і загрозам, що виникають внаслідок фундаментальних політичних,

економічних і науково-технологічних зрушень. Найбільш небезпечною тенденцією стало зростання масштабів використання методів гібридного протиборства, які відрізняються гнучкістю, комплексністю, багатосуб'єктністю, багатоакторністю. Водночас, у поєднанні із засобами інформаційного протиборства та кібервійни, інформаційно-психологічними операціями, пропагандистськими кампаніями, масштабним поширенням дезінформації та фейків через глобальні засоби масової інформації, методи гібридної війни демонструють високий рівень ефективності у досягненні цілей агресії, дозволяючи уникати масштабного застосування конвенційних озброєнь. Саме тому вони набули популярності не тільки серед держав, але й різноманітних недержавних акторів – терористичних та екстремістських об'єднань, злочинних угруповань, окремо діючих осіб.

Найбільш динамічним простором для здійснення гібридної агресії виступають соціальні медіа, платформи та месенджери, які мають цілу низку переваг у порівняні з іншими вимірами протистояння – масштабність охоплення аудиторії, доступність, швидкість поширення інформації, анонімність, можливість обміну великим масивом даних, відсутність географічних або змістових обмежень для діяльності. Facebook / Meta, YouTube, Instagram, WeChat, TikTok, Twitter, WhatsApp, Messenger Facebook, Telegram, Snapchat стали не тільки найбільш популярними соціальними медіа та месенджерами, але й ефективним інструментом для збору необхідної інформації стратегічного і тактичного характеру, виявлення потенційних цілей для подальших дій у фізичному просторі, здійснення кібератак та інформаційно-психологічних впливів на свідомість користувачів, спілкування, вербування нових членів та координації діяльності повстанських груп, терористичних угруповань, екстремістських об'єднань та кримінальних організацій.

Особливого значення соціальні медіа, платформи та месенджери набули у контексті гібридної війни РФ проти України, яка активно велася з 2014 р. Російські пропагандистські наративи, фейки, дезінформація активно поширювалися не тільки традиційними ЗМІ, але й соціальними медіа, що уможливило проведення масштабної інформаційної війни проти української держави. Із початком відкритої військової агресії у лютому 2022 р. соціальні медіа як інструмент гібридної війни не втратили своєї актуальності, а стали складовою інформаційного супроводження воєнної кампанії.

Аналіз попередніх досліджень. Дослідження інформаційного виміру гібридної війни представлено роботами провідних фахівців у сфері інформаційного протиборства та використання сучасних засобів масової інформації і комунікації у гібридних війнах і конфліктах, зокрема, Дж. Меттіса (Mattis & Hoffman, 2005), Ф. Хоффмана (Hoffman, 2009), Р. Шафранскі (Szafranski, 1995), М. Лібікі (Libicki, 2009, 2012), Д. Стейна (Stein, 1995), Дж. Ная (Nye, 2010, 2011), Д. Арквілли, Д. Ронфельдта (Arquilla & Ronfeldt, 1993), П. Померанцева (Pomerantsev, 2020), Е. Тоффлера та Г. Тоффлер (Toffler & Тоффлер, 1995), М. ван Кревельда (Creveld, 1991), Р. Ендрес (Andres, 2014) та ін. Питання вепонізації соціальних медіа, використання методів Інтернет-тролінгу, а також використання терористичними організаціями соціальних мереж досліджувалося в наукових працях П.В. Сінгера, Е.Т. Брукінга (Singer & Brooking, 2019), Т.Е. Ніссена (Nissen, 2015), Т. Хоквалда (Hochwald, 2023), С. Светоки, А. Рейнолдс і Л. Куріки (Svetoka & Reynolds, 2016), А. Спрудса, А. Рожукалне, К. Седленієкс, М. Даугуліс (Spruds, Rožukalne, Sedlenieks et al., 2016) та ін.

Особливу увагу у роботах українських науковців та експертів приділено проблемам інформаційного, психологічного та ідеологічного вимірів гібридного протистояння. Зокрема, у працях В. Горбуліна (Horbulin, 2017), Г. Почепцова (Pocheptsov, 2015, 2017, 2019a; 2019b), Д. Дубова (Dubov, 2014), М. Ожевана, (Ozhevan & Dubov, 2017), Є. Магди (Magda, 2014), М. Бєлескова (Бєлєсков, 2021), Г. Яворської (Yavorska, 2018), О. Курбана (Kurban, 2016, 2017), Т. Ісакової (Isakova, 2016) та ін. розглядаються питання гібридної війни як новітньої форми глобального

протистояння у сучасній системі безпеки, появи нових характерних рис сучасної гібридної війни у світі та Україні, особливості використання різних класичних та інноваційних інструментів гібридної війни в українських реаліях, а також практики використання інформаційних, інформаційно-психологічних, кібернетичних засобів ведення гібридної війни РФ проти Україною.

Метою статті є дослідження теоретичних і прикладних аспектів використання соціальних медіа як ефективного інструменту гібридної війни у сучасному світі.

Виклад основного матеріалу. Прискорений розвиток інформаційно-комунікаційних технологій призвів до масштабних змін в усіх сферах життєдіяльності людини. Нові можливості відкрилися у сфері економіки, бізнесу і фінансів, з'явилися сучасні моделі економічної діяльності, змінилися підходи до управління державою, швидкими темпами відбуваються зміни у сфері суспільного розвитку. Позитивний ефект постійно підсилюється появою нових технологічних досягнень в рамках реалізації проєктів розбудови Індустрії 5.0. Водночас, розвиток технологій призвів до появи нових викликів і загроз для безпеки сучасного суспільства: змінилася природа конфліктів, суттєво ускладнилися традиційні простори ведення бойових дій, з'явилися нові засоби протиборства, що базуються на досягненнях у сфері науки і технологій. До того ж глобальний доступ до віртуального середовища призвів до виникнення віртуального поля бою, інтелектуальних бійців, які використовують інформаційну зброю. Об'єктами атак в сучасних війнах і конфліктах дедалі частіше стають кіберфізичні системи, де технології можуть впливати як на фізичний простір існування людини, так й на її когнітивну діяльність, а отже й наслідки застосування інформаційних методів протиборства можуть мати летальний характер для людини.

Останнім часом як держави, так і недержавні актори активно використовують гібридні підходи для досягнення своїх політичних і воєнних цілей, вміло поєднуючи військові операції з кібератаками, дипломатичним або економічним тиском та інформаційно-психологічними і пропагандистськими кампаніями. В цьому контексті особливого значення набувають соціальні медіа, які за останнє десятиліття перетворилися на один з основних каналів комунікації, що використовується у всіх сферах життєдіяльності людини. Віртуальні Інтернет-ресурси стали не тільки невід'ємною частиною сучасного суспільства, але й новітніх стратегій ведення війни. Останні конфлікти в Лівії, Сирії та Україні продемонстрували, що соціальні медіа широко використовуються для координації дій, збору інформації, впливу на переконання та настрої цільових аудиторій, мобілізуючи їх до дії.

До основних переваг використання соціальних мереж можна віднести їх масштаб охоплення аудиторії, доступність, швидкість розповсюдження інформації, анонімність, можливість обміну великим обсягом інформації, відсутність географічних або змістових кордонів. Так, станом на початок 2023 рр. загальна чисельність користувачів Інтернетом перевісила 5 млрд. осіб, що становить близько 64,4% від усього населення світу. При цьому соціальними медіа користувалося 4, 76 млрд. осіб, що становить близько 60% від загальної кількості населення Землі. Найбільш популярними соціальними медіа є Facebook / Meta, YouTube, Instagram, WeChat, TikTok, Twitter, месенджерами – WhatsApp, Messenger Facebook, Telegram, Snapchat (Kemp, January 26, 2023). Можливості знімати, редагувати та обмінюватися інформацією, зображеннями та відео в режимі реального часу, незалежно від того, чи повідомляють традиційні ЗМІ про події чи ні, а також можливості охопити якомога більшу аудиторію для здійснення масштабних інформаційних кампаній дезінформації та агресивної пропаганди, інформаційно-психологічних операцій робить соціальні медіа надзвичайно ефективним інструментом гібридної війни.

На думку Т.Е. Ніссена, основними способами використання соціальних медіа у гібридній війні є:

- ❖ збір розвідданих – передбачає цілеспрямований пошук і аналіз інформації

в соціальних мережах і профілях користувачів, включаючи вміст і розмови, що допомагає більш успішному проведенню воєнної операції із врахуванням особливостей інформаційного середовища, цільової аудиторії, на яку передусім розрахований вплив;

❖ таргетинг – використання соціальних медіа з метою виявлення потенційних цілей для військових дій у фізичному просторі (на основі фотографій із геотегами чи поточних розмов у соціальних мережах);

❖ інформаційно-психологічна війна – поширення інформації з метою впливу на цінності, систему переконань, сприйняття, емоції, мотивацію, міркування та поведінку цільової аудиторії (використання соціальних мереж у цьому випадку спрямоване на досягнення певних військових ефектів у когнітивній сфері, що досягається шляхом створення офіційних акаунтів, каналів, сайтів, коментарів лідерів думок, а також шляхом створенная фейкових облікових записів користувачів, ботнетів та тролінгу);

❖ кібероперації – сукупність дій, спрямованих на платформи соціальних медіа та облікові записи їх користувачів з метою зламу захищених паролем просторів для отримання доступу та розкриття вмісту чатів, електронної пошти чи мобільних телефонів, зміни вмісту профілю тощо;

❖ оборона – діяльність із захисту платформ соціальних мереж, сайтів, профілів і облікових записів на технічному або системному рівні, що включає використання програмного забезпечення для шифрування, відстеження та/або приховування IP-адрес у соціальних мережах (наприклад, використання однією з найскладніших ігрових платформ для відстеження правоохоронними органами PlayStation);

❖ командування та управління – використання соціальних медіа повстанськими групами, терористичними угрупованнями, кримінальними організаціями, особливо якщо ці групи не мають формальної структури або розосереджені на великих географічних територіях. Соціальні медіа можуть бути засобом спілкування та способом координації їхньої діяльності, що робить їх привабливим механізмом для використання під час гібридних війн і тому привертає увагу спецслужб. Соціальні медіа також використовуються для тактики «роїння» – розповсюдження інформації для мобілізації та координації недержавних акторів зі спільними інтересами для взаємодії з конкретною ціллю, що також уможливлює їх широке використання у гібридній війні (Nissen, 2015: 70-83).

Усі перелічені способи використання соціальних медіа можуть взаємодоповнювати один одного у довільних і непередбачуваних комбінаціях, а також можуть поєднуватися із реальними військовими операціями під час здійснення гібридних атак.

Наукові дискусії щодо використання соціальних мереж у гібридних війнах призвели до виникнення поняття «соціальні кібератаки», які тлумачаться як навмисні та організовані дії з поширення чуток, містифікацій та маніпулятивних повідомлень у віртуальному середовищі, спрямовані на те, щоб викликати страх і паніку. Оскільки відстежити організаторів і виконавців соціальних кібератак складно, вони залишаються анонімними, приховуючи як реальних людей, які стоять за атаками, так й автоматизовані мережі ботів. Наприклад, у липні 2012 р. в індійському штаті Ассам було поширено фальшиві зображення і текстові повідомлення про напади на мусульманське населення, що призвело до панічної масової втечі громадян з місця проживання (Hasan, September 3, 2012).

Під час проведення гібридної війни з використанням соціальних мереж використовуються й інші методи і прийоми для психологічного впливу та маніпуляції, зокрема: поширення автоматично згенерованого контенту, спаму (наприклад, «твіттер-бомби» – розсилка тисяч схожих повідомлень одночасно) або фейкових ідентифікацій (наприклад, за допомогою діяльності тролів, маріонеток, ботів); насичення інформаційного простору шляхом скоординованого використання

блогів, постів, статей тощо, які публікуються та репостяться лідерами думок, активістами та фейковими особами; викрадення популярних хеш-тегів у Twitter з метою збільшення охоплення повідомлення або перенаправлення аудиторії (наприклад, #napaquake, #WorldCup2014); атака на цільовий контент супротивника, що передбачає його блокування, звернення до адміністраторів і менеджерів соціальних медіа-платформ з вимогою видалити вміст певних профілів, скарги на неприйнятний контент (наприклад, адміністрація Facebook видалила фотографію дівчинки, яка вшановує пам'ять свого батька – українського солдата, який загинув на сході України, після того, як кілька проросійських користувачів соціальних мереж повідомили про те, що публікація містить неприйнятний контент і сцени насильства); таргетинг передбачає використання різних стратегій нападу на опонента з метою отримання персональної інформації та використання її для дискредитації, висміювання, погроз тощо; соціальна інженерія як складова інформаційного виміру гібридного протиборства відноситься до психологічного маніпулювання людьми з метою примусити їх виконувати певні дії або розголошувати конфіденційну інформацію; обман, що передбачає створення «шуму» або «інформаційного туману» навколо теми з метою відволікання уваги від більш стратегічно важливих подій (наприклад, після збиття малайзійського літака рейсу MH17 російські медіа-канали та соціальні мережі розповсюдили велику кількість повідомлень, які пропонували численні пояснення причин катастрофи літака) (Svetoka et al., 2016: 18-20).

Активно використовується також й технології «астротурфінгу», який тлумачиться як імітація масової громадської ініціативи для створення ілюзії запиту від суспільства. Для цього використовуються соціальні мережі, коментарі у різних медіа, масова розсилка повідомлень, звернення та петиції, а також діяльність інфлюенсерів. Ключовим інструментом астротурфінгу виступають цифрові технології ботоферм, які імітують масову народну реакцію або ініціативу (Svetoka et al., 2016: 27).

Іншою технологією є Інтернет-тролінг, який широко використовується в гібридному протистоянні для маніпулювання думкою людей шляхом поширення пропаганди та чуток, провокування онлайн-дискусії внаслідок нападок на коментаторів з альтернативними поглядами. Нині, в умовах зростання актуальності проблеми використання інструментів гібридної війни у протиборстві держав, з'явився новий тип тролів – «гібридні тролі», які використовують ті ж моделі поведінки, що і традиційні, але діють в певному політичному контексті або рамках військового порядку денного. Гібридні тролі поширюють певну ідеологію і, що найголовніше, діють під керівництвом і за наказом конкретної держави або організації. Наприклад, такі тролі активно використовуються РФ у гібридному протистоянні з Україною, іншими країнами пострадянського простору та країнами Заходу, поширюючи повідомлення та коментарі проросійського змісту у соціальних мережах. Найчастіше, у випадку появи інформації про події в Україні, відбувається синхронізована масована атака на новини і пости в блогах, наростає обсяг коментарів у соціальних мережах одночасно в багатьох країнах світу (Spruds et al, 2016).

Цілі та зміст повідомлень гібридних тролів можуть відрізнятися в різних країнах, залежно від конкретних цільових аудиторій. Так, за даними польських дослідників, які проаналізували методи соціального впливу на прикладі аналізу повідомлень щодо агресії РФ проти України у соціальних мережах, комунікаційні стратегії гібридних тролів мають суттєві відмінності. Тролі, які пишуть російською мовою, беруть участь у дискусіях, щоб заспокоїти учасників, приховати правду про стан російської економіки і вихваляти чесноти президента та уряду РФ; тролі, які пишуть українською мовою, використовують свої коментарі для дискредитації та приниження Президента та уряду України, зображуючи їхні дії як ворожі та зневажливі, а також порівнюючи їх з фашистами; тролі, які пишуть польською

мовою, намагаються переконати Інтернет-користувачів, що війна в Україні – це не справа поляків, а також використовують суперечливі аргументи щодо спільної історії України та Польщі, щоб представити українців у якомога гіршому світлі (Svetoka et al., 2016: 43-45)

Слід зазначити, що різноманітні соціальні медіа і месенджери активно використовувалися у гібридній війні РФ проти України від тоді, як вони почали набувати популярності в українському суспільстві і перетворюватися на важливий засіб комунікації. Так, ще у 2014 р. під час подій на «Майдані» саме в Інтернеті, у тому числі через соціальні медіа і платформи, поширювалася інформація, за допомогою якої РФ та представники проросійського уряду України намагалися дискредитувати учасників масової акції протесту. Упродовж усього періоду з 2014 р. по 2022 р. соціальні медіа використовувалися російськими пропагандистськими ЗМІ для збільшення аудиторії та спрощення донесення маніпулятивної та брехливої інформації до споживачів як у самій Росії, так й в Україні та світі. Із початком військової агресії РФ проти України популярність соціальних медіа і месенджерів як засобу отримання і обміну інформацією суттєво зросла. Так, за даними досліджень від 74% до 76,6% населення є постійними користувачами різноманітних соціальних медіа, платформ і месенджерів. При цьому 93,5% Інтернет-користувачів використовують принаймні одну соціальну платформу (Kemp, February 14, 2023). Найбільш популярними є Telegram, YouTube і Facebook.

Слід зазначити, що поширення практики використання відеохостінгу Youtube для здійснення пропагандистської діяльності було обумовлене тим, що платформа від початку позиціонувала себе як віртуальне середовище, де кожен має право висловити свою думку та можливість показати власне бачення світу іншим учасникам онлайн-спільноти, виробникам контенту та споживачам інформації. Цим користується російська пропаганда, яка поширює дезінформацію, розпалює ненависть, використовує геноцидну риторику проти українського народу для того, щоб з 2014 р. легітимізувати окупацію частини української території та анексію Криму, а з 2022 р. – воєнні злочини російських військових в Україні. Наприклад, ще до початку повномасштабної війни проти України російські провладні Youtube-канали та онлайн-ресурси, що належать підконтрольним Москві квазіутворенням «ДНР» та «ЛНР», активно використовували платформу для поширення проросійської пропаганди та дезінформації попри суворі правила цензури, не блокувались і навіть не мали дисклеймерів (Nesterenko, May 16, 2023). Наразі нараховується понад 46 російських та проросійських Youtube-каналів, що діють на українську та закордонну аудиторію. З метою попередження або обмеження деструктивного впливу російських пропагандистських ресурсів з 2022 р. Службою безпеки України було заблоковано 442 пропагандистських Youtube-каналів РФ, зокрема, «Первый канал», «Телеканал «Звезда», RT, «Соловьев LIVE». Водночас, контент усіх цих каналів й досі можна знайти у YouTube і подивитися навіть без використання VPN, оскільки часто їх продукти «перезаливаються» на інші, не пов'язані з офіційними російськими ЗМІК, ресурси (Bor do, Mor2 та ін.). Діяльність таких каналів є не менш небезпечною, ніж офіційних, оскільки вони постійно оновлюють контент, що містить фейки, образливі висловлювання на адресу українських і західних політиків, кремлівські наративи про нелегітимність української влади, яку вони називають «київський режим», про те, що Україна бомбить сама себе і своїх громадян, про зовнішнє управління та несамостійність української держави, упереджену інтерпретацію історичного розвитку України тощо. Загалом щонайменше вісім пропагандистських каналів РФ на YouTube, незважаючи на санкції, продовжують поширювати свій контент на відеохостингу, бо досі не потрапили під блокування або заблоковані некоректно (зокрема, «Московский комсомолец», «Комсомольская правда», телеканал, що перебуває у власності міноборони Росії, «Звезда» (доступний на YouTube, зокрема для громадян України, під назвою Zvezda Live 10.0.) (Nesterenko, May 16, 2023).

За допомогою як класичних, так й новітніх прийомів пропаганди та дезінформації, поширюються вже відомі наративи, в яких Росія представляється як справедлива, сильна і незалежна держава, яка реалізує місіонерські цілі, а не здійснює експансію. Так, на YouTube-каналі КОНТ, на який підписані 245 тисяч людей, розміщується різноманітний контент, який є по суті архівом програм пропагандистів Д. Кисельова та О. Пушкова. Саме на цьому ресурсі був розміщений відомий провокаційний ролик «Я – російський окупант» («I'm a Russian Occupant»), в якому йдеться про позитивні результати окупації росіянами території сучасного Сибіру, країн Балтії і Середньої Азії, а також України. Наприкінці відео закадровий голос говорить, що востаннє ввічливо попереджає, щоб інші «не наривалися», що «руський окупант» «любить мир, будує мир, а воювати він вміє краще за всіх». Дане відео набрало на YouTube понад 357 тис. переглядів (I'm a Russian Occupant, 2015).

Показовим прикладом інформаційної атаки у YouTube є поширення відео з провокативною назвою «Zelensky is the black hole». На платформі спочатку з'явився ролик, де ведучі регіональних новин штату Мічиган «WDIV-TV» нібито пропонують глядачам послухати звуки чорної діри, натомість на екрані з'явилося звернення В. Зеленського. Як з'ясувалося згодом, насправді це був фейк, а на американському телебаченні такого ніколи не транслювали. Продовженням даного фейку стало інше відео з написом «No Zelensky. No War», яке нібито з'явилося замість реклами на площі Таймс-сквер у Нью-Йорку. Цю дезінформацію було оперативно спростовано МЗС України та Генеральним Консульством України у Нью-Йорку, а згодом спростування з'явилося й у мережі. Основною метою таких роликів є дискредитація української влади і створення ілюзії, буцімто світ втомився від України, що саме Україна прагне війни, а міжнародні партнери вже почали відгортатися від української держави («Black hole» 2.0, 2023).

Російські пропагандистські ЗМІК активно використовують сучасні інструменти, зокрема, діпфейки, монтаж та фотошоп. Прикладом такої діяльності є поширення у березні 2022 р. діпфейку у соціальних медіа та месенджерах, які розмістили брехливу інформацію із начебто заявою президента В. Зеленського із закликом до українських громадян і військових припинити супротив та скласти зброю. Спочатку це відео з'явилося на веб-сайті з сумнівною репутацією, а потім його почали поширювати соціальні платформи і медіа – Facebook, Instagram, YouTube та проросійські Телеграм-канали (Wakefield, March 18, 2022).

Значну небезпеку становлять також YouTube-канали підконтрольних Кремлю квазіутворень «ЛНР» та «ДНР», а також інформаційні ресурси, створені на території тимчасово окупованого Криму – YouTube-канали «Новороссия ТВ», «АРХІВ НОВОРОССИЯ ТВ», «(Z) Новости СВО Видео», «Za Донбасс» (телеканал Юнион), «Трибунал ДНР», Millet Channel. Вони не тільки постійно поширюють фейкові новини, дезінформацію та антиукраїнську інформацію, а й користуються політикою платформи для представлення свого контенту як альтернативної думки іншої сторони, що робить їх складовою гібридної війни РФ проти України. При цьому значна частина цих ресурсів містить кадри з тілами вбитих чи закатованих цивільних українців, поранених і скалічених військових полонених, відео катування українських військовополонених та інтерв'ю з ними, що однозначно відноситься до категорії забороненого контенту вразливого чи насильницького характеру. Водночас, ці канали не тільки не блокуються YouTube, але іноді не мають навіть дисклеймери про потенційно шкідливий контент (Nesterenko, May 16, 2023).

У гібридній війні проти України використовуються також іноземні медіа та журналісти, які відвідують Донбас і окупований Крим з метою пошуку «істини» та «почути іншу думку». Результатом такої діяльності є поява в інформаційному просторі України та світу контенту, що суперечить не тільки офіційним даним, наданим Україною, а й підтвердженим міжнародними експертами фактам. Наприклад, у відеосюжетах медіа-ресурсу VICE, розміщених на платформі YouTube, повторюються прокремлівські пропагандистські наративи, демонструються інтерв'ю

з проросійсько налаштованими мешканцями окупованого Криму та представниками квазіутворень «ЛНР» та «ДНР», демонструються сцени насильства під час захоплення території Донбасу. При цьому більшість відео можна дивитися без обмежень (Life Inside Putin's Crimea, December 9, 2019; Rebels Retreat To Donetsk, July 10, 2014; The Donetsk People's Republic, October 8, 2014).

На початку лютого 2022 р. журналісти французького телевізійного каналу TF1 відвідали територію ОРДЛО, перетнувши кордон з боку Росії через пункт пропуску Ізварино, і спілкувалися з ватажком бойовиків Д. Пушиліним (French journalists illegally went…, February 14, 2022). У лютому 2023 р. виник новий скандал, після появи репортажу американських журналістів NBC News, які відвідали окупований Крим, в'їхавши на нього через Керченській міст, порушивши закони України (See inside Crimea, February 28, 2023). У відеосюжеті йдеться про військові дії на Сході України і про Крим, який для Кремля є «червоною лінією», після порушення якої відбудеться «жорстка відповідь» Москви.

Важливу роль у поширенні пропагандистської інформації російськими ЗМІК відіграє Telegram, який виступає дієвим інструментом гібридної війни. На відміну від YouTube, політика аналізу контенту Telegram набагато лояльніша, а модерація – обмежена, що дозволяє безперешкодно поширювати фейки, дезінформацію, упереджену інформацію та здійснювати різні типи маніпулятивних стратегій. Наприклад, матеріали пропагандистського характеру, розміщені на ресурсах, пов'язаних з російськими державними ЗМІ, завантажуються безпосередньо в Telegram. При цьому відеоматеріали перекладаються 18 мовами, що дозволяє охоплювати не тільки російськомовну та україномовну аудиторію, але й аудиторії різних країн світу. Далі відео може бути повторно опубліковано на інших соціальних платформах, зокрема, Twitter, без позначення першоджерела інформації та вказівок на те, що відео створено російськими пропагандистськими ЗМІ.

Такі ресурси просувають пропагандистські наративи, концептуальні позиції, характерні для політики Кремля, звинувачення України у провокації початку агресії та у жертвах серед цивільного населення, а також фейки про начебто очікування місцевого населення на прихід росіян. До того ж відео можна завантажити безпосередньо з Telegram, що приховує сліди, за якими експерти могли б відстежити походження цих ресурсів. Російські пропагандисти виявляють креативність і адаптивність, вони ретельно вивчають свою цільову аудиторію, щоб адаптувати до неї потрібний контент (Klepper, October 5, 2022).

Telegram-канали можуть також слугувати своєрідним сховищем відео для російського пропагандистського контенту, пов'язаного з війною в Україні. (Russian's RT, 2022). Кожне відео має субтитри мовою оригіналу та субтитри іншими мовами з хештегами, які використовуються для організації багатомовної роботи з метою подальшого поширення інформації в соціальних медіа. У деяких випадках водяні знаки, які ідентифікували б відео як таке, що створено підсанкційними ЗМІК, можуть бути видалені з метою маскування джерела їх походження. Далі ж, потрапивши до Telegram, відео завантажуються та повторно публікуються на інших цифрових платформах, включаючи Twitter, без жодних позначок чи інших ознак того, що відео, наприклад, створено російськими державними ЗМІ.

Із початком агресії РФ проти України проросійські акаунти Telegram поширювали антиукраїнський контент традиційними методами дезінформації та використання ботів. Найбільш активними у поширенні прокремлівської пропаганди, дезінформації та фейків нині є так звані російські воєнкори, які знімають репортажі з місця бойових дій, показуючи переваги і досягнення російської армії, створюючи ілюзію непереможності, стійкості та близької перемоги в СВО.

Окрім реальних російських військових кореспондентів останнім часом з'явилися фейкові акаунти, власники яких видають себе за них і, користуючись підтримкою мережі прокремлівських каналів, маскують свій контент під об'єктивні репортажі з місця подій. Часто вони використовують ефекти спеціальної зйомки, що

імітує «бойову обстановку» – різко смикають камеру, збивають з фокусу, знімають людей, які кудись біжать, додають аудіоефекти – звуки вибухів, вистрілів або криків. Все це створює ефект реального перебування на місці подій, ілюзії страшної дійсності, що й потрібно пропагандистам для надання реалістичності картинки. Наприклад, російський Telegram-канал «Війна з фейками», який видає себе за сервіс перевірки фактів про «конфлікт на Україні», поширює дезінформацію та пропаганду серед своєї аудиторії, яка постійно зростає і нині вже налічує понад 630 тис. підписників (Bergengruen, March 21, 2022).

Висновки. Таким чином, як свідчить проведений аналіз, соціальні медіа, платформи і месенджери перетворилися на ефективний і динамічний простір протистояння у сучасних гібридних війнах і конфліктах. Основними перевагами Інтернет-сервісів є масштабність охоплення користувачів, доступність, анонімність, можливість обміну великими даними незалежно від кордонів тощо, що призвело до швидкого зростання їх популярності серед населення різних країн і регіонів світу. Водночас, ці ж характеристики роблять їх надзвичайно ефективним інструментом гібридних воєн і дозволяють як традиційним, так і не традиційним учасникам протиборства збирати необхідну інформацію стратегічного і тактичного характеру для планування і здійснення операцій, виявляти потенційні цілі для подальших дій у фізичному просторі, здійснювати різноманітні кібератаки на критичні елементи інфраструктури держав, проводити інформаційно-психологічні операції, вербувати нових членів та координації діяльності повстанських груп, терористичних угруповань, екстремістських об'єднань та кримінальних організацій.

Для досягнення поставлених цілей активно використовуються різноманітні методи здійснення атак через соціальні медіа, зокрема, соціальні кібератаки та соціальна інженерія, використання автоматично згенерованого контенту, спаму або фейкових ідентифікацій, скоординоване використання блогів, постів, статей; викрадення популярних хеш-тегів; атака на цільовий контент супротивника; таргетинг опонента; створення «шуму» або «інформаційного туману»; астротурфінг та Інтернет-тролінг.

Соціальні медіа та месенджери активно використовуються як інструмент гібридної війни РФ проти України починаючи з 2014 р. Російські пропагандистські ЗМІ використовували їх як ефективний канал вплив на українську та світову аудиторію, поширюючи брехливу інформацію з метою дискредитації України, її уряду та Збройних сил, а також легітимізації окупації частини території та анексії Криму.

References

Andres, R.B. (2014). Inverted-militarized-diplomacy: how states bargain with cyber weapons. *Georgetown Journal of International Affairs. International Engagement on Cyber Weapons.*

Arquilla, J. & Ronfeldt, D. (1993). *Cyberwar is Coming!* Retrieved from https://cutt.ly/jwWv2Z1Q

Barovska, A. & Dubov, D. (2018). Strategic Communications in Hybrid War: conceptual and theoretical understanding. *Strategic communications in hybrid warfare: from volunteer to scientist: monograph*. Kyiv: NA SB Ukrainy, 19-48 // **Баровська, А. & Дубов, Д.** (2018). Стратегічні Комунікації в Гібридній Війні: концептуальне і теоретичне осмислення. Стратегічні комунікації в умовах гібридної війни: від волонтера до науковця: монографія. Київ: НА СБ України, 19-48.

Bergengruen, V. (March 21, 2022). How Telegram Became the Digital Battlefield in the Russia-Ukraine War. *Time*. Retrieved from https://cutt.ly/9wWv792S

Bielieskov, M.M. (2021). The modern Russian way of waging war: theoretical foundations and practical content. Analytical report. *NISS*. Retrieved from https://cutt.ly/WwWv94KF // **Бєлєсков, М.М.** (2021). Сучасний російський спосіб ведення війни: теоретичні основи і практичне наповнення. Аналітична доповідь. *НІСД*. Retrieved from https://cutt.ly/WwWv94KF

«Black hole» 2.0: propahanda rf poshyriuie feik pro baner iz Zelenskym u Niu-Yorku (2023). *Center for Countering Disinformation*. Retrieved from https://cutt.ly/VwWv38P9 // «Black hole» 2.0: пропаганда рф поширюйте фейк про банер із Зеленським у Нью-Йорку (2023). Центр протидії дезінформації. Retrieved from https://cutt.ly/VwWv38P9

Creveld, M.V. (1991). *The Transformation of War*. New York: Free Press.

Dubov, D.V. (2014). Cyberspace as a new dimension of geopolitical rivalry. Kyiv: NISS // **Дубов, Д.В.** (2014). Кіберпростір як новий вимір геополітичного суперництва. Київ: НІСД.

French journalists illegally went to Donbas to see the leader of the "DNR" Pushylin (February 14, 2022). *NV New Voice*. Retrieved from https://cutt.ly/nwWv8QZ2 // Французькі журналісти незаконно з'їздили на Донбас до ватажка «ДНР» Пушиліна (February 14, 2022). *NV New Voice*. Retrieved from https://cutt.ly/nwWv8QZ2

Hasan, A. (September 3, 2012). Why the violence in Assam is not communal. *BBC News*. Retrieved from https://cutt.ly/SwWv3ACI

Hochwald, T. (2023). How Do Social Media Affect Intra-State Conflicts other than War? *Connections: The Quarterly Journal*. Retrieved from https://cutt.ly/ZwWv9VVP

Hoffman, F.G. (2009). Hybrid Warfare and Challenges. *JFO,* 52 (1), 34-39. Retrieved from https://cutt.ly/owWv9UxF

Horbulin, V. (2017). The world hybrid war: Ukrainian Forefront. Kharkiv: «Folio».

Isakova, T., Hnatiuk, S., Dubov, D., Chernenko, T. & Barovska, A. (2016). *Information Challenges of Hybrid Warfare: Content, Channels, Countermeasures: Analytical Report*. Kyiv: NISS. Retrieved from https://cutt.ly/cwWv3pLz // **Ісакова, Т., Гнатюк, С., Дубов, Д., Черненко, Т. & Баровська, А.** (2016). *Інформаційні виклики гібридної війни: контент, канали, механізми протидії: аналітична доповідь*. Київ: НІСД. Retrieved from https://cutt.ly/cwWv3pLz

Kemp, S. (January 26, 2023). Digital 2023: Global overview report. *Datareportal* Retrieved from https://cutt.ly/RwWv3Qwx

Kemp, S. (February 14, 2023). Digital 2023: Ukraine. *Datareportal* Retrieved from https://cutt.ly/cwWv3Ylv

Klepper, D. (October 5, 2022). Experts: Russia finding new ways to spread propaganda videos. *AP*. Retrieved from https://cutt.ly/9wWv7DXg

Kurban, O. (January 19, 2016). Hybrid warfare: special operations forces and social networks. *Rakurs*. Retrieved from https://cutt.ly/ywWv3lHQ // **Курбан, О.** (January 19, 2016). Гібридна війна: сили спецоперації та соціальні мережі. *Ракурс*. Retrieved from https://cutt.ly/ywWv3lHQ

Kurban, O. (February 3, 2017). Network weapons of mass destruction: technology and the human factor. *Rakurs*. Retrieved from https://cutt.ly/owWv3gm2 // **Курбан, О.** (2017). Мережева зброя масового ураження: технології та людський фактор. *Ракурс*. Retrieved from https://cutt.ly/owWv3gm2

Libicki, M.C. (2009). *Cyberdeterrence and Cyberwar*. RAND. Retrieved from https://cutt.ly/cwWv2O7J

Libicki, M.C. (2012). Cyberspace Is Not a Warfighting Domain. *A Journal of Law and Policy for the Information society*, 8 (2), 321-336. Retrieved from https://cutt.ly/cwWv2Gb7

Life Inside Putin's Crimea (December 9, 2019). *VICE News*. Retrieved from https://cutt.ly/xwWv8uvZ

Magda Y.V. (2014). The Challenges of Hybrid Warfare: Information Aspect. *Naukovi zapysky Instytutu zakonodavstva Verkhovnoi Rady Ukrainy*, 5, 138-142. Retrieved from https://cutt.ly/ywWv99EU // **Магда, Ю.В.** (2014). Виклики гібридної війни: інформаційний вимір. Наукові записки Інституту законодавства Верховної Ради України, 5, 138-142. Retrieved from https://cutt.ly/ywWv99EU

Mattis, J.N. & Hoffman, F.G. (2005). Future Warfare: The Rise of Hybrid Wars. *Proceedings Magazine*. Retrieved from https://cutt.ly/EwWv205P

Nesterenko, A. (May 16, 2023). Corpses, racism and war criminals: which Russian channels has YouTube not blocked yet? *Instytut masovoi informatsii*. Retrieved from https://cutt.ly/MwWv3HXq // **Нестеренко, А.** (May 16, 2023). Трупи, рашизм та воєнні злочинці: які російські канали досі не заблокував Youtube? *Інститут масової інформації*. Retrieved from https://cutt.ly/MwWv3HXq

Nissen, T.E. (2015). *The Weaponization Of Social Media: Characteristics of Contemporary Conflicts*. Copenhagen: Royal Danish Defence College.

Nye, J.S. (2010). *Cyber Power*. Cambridge: Harvard Kennedy School. Retrieved from https://cutt.ly/8wWv2Nlj

Nye, J.S. (2011). *The Future of Power*. New York: PublicAffairs.

Ozhevan, M.A. & Dubov, D.V. (2017). *Homo ex Machina. Philosophical, cultural and political prerequisites for the formation of a convergent society*. Kyiv: NISS // **Ожеван, М.А. & Дубов, Д.В.** (2017). *Homo ex Machina. Філософські, культурологічні та політичні передумови формування конвергентного суспільства*. Київ: НІСД.

Pocheptsov, H. (2017). From pokemon to hybrid wars. New communication technologies of the 21st century. Kyiv: Vydavnychii dim «Kyievo-Mohylianska akademiia» // **Почепцов, Г.** (2017). Від покемонії до гібридних війн. Нові комунікативні технології XXI століття. Київ: Видавничий дім «Києво-Могилянська академія».

Pocheptsov, H. (2019). *Cognitive wars in social media, mass culture and mass communications*. Kharkov: Folio // **Почепцов, Г.** (2019). *Когнитивные войны в соцмедиа, массовой культуре и массовых коммуникациях*. Харьков: Фолио.

Pocheptsov, H. (2019). *Virtual wars. Fakes*. Kharkov: Folio // **Почепцов, Г.** (2019). *Виртуальные войны. Фейки*. Харьков: Фолио.

Pomerantsev, P. (2020). *This is not propaganda. A journey to war against reality*. Kyiv: Yakaboo Publishing // **Померанцев, П.** (2020). *Це не пропаганда. Подорож на війну проти реальності*. Київ: Yakaboo Publishing

*Rebels Retreat To Donetsk: Russian Roulette (*July 10, *2014). VICE News*. Retrieved from https://cutt.ly/CwWv8sWS

Russian's RT Leads a Global "Information Militia" on Social Media to Bypass Censorship on Ukraine-Related Disinformation. An Investigative Report (October 5, 2022). *NISOS*. Retrieved from https://cutt.ly/swWv7CSE

See inside Crimea as Ukraine hopes to retake the Russian-annexed territory (February 28, 2023). *NBC News*. Retrieved from February https://cutt.ly/XwWv8UTT

Singer, P.W. & Brooking, E.T. (2018). *LikeWar. The Weaponization of Social Media*. New York: Houghton Mifflin Harcourt

Spruds, A., Rožukalne, A., Sedlenieks, K., Daugulis, M., Potjomkina, D., Tölgyesi, B. & Bruge, I. (2016). *Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia*. Riga: Latvian Institute of International Affairs Stradins University / NATO StratCom COE. Retrieved from https://cutt.ly/AwWv9K4k

Stein, G. (1995). Information Warfare. *Airpower Journal*. Retrieved from https://cutt.ly/ZwWv2TmH

Svetoka, S., Reynolds, A. & Curika, L. (2016). *Social Media as a Tool of Hybrid Warfare*. Riga: NATO Strategic Communications Centre of Excellence. Retrieved from https://cutt.ly/vwWv9S9M

Szafranski, R. (1995). A theory of information warfare. *Airpower Journal*. Retrieved from https://cutt.ly/dwWv2paP

The Donetsk People's Republic (October 8, 2014). *VICE News*. Retrieved from https://cutt.ly/SwWv8hG7

Toffler, A. & Toffler, H. (1995). *War and Anti-war*. New York: Warner Books

Wakefield, J. (March 18, 2022). Deepfake presidents used in Russia-Ukraine war. BBC News. Retrieved from https://cutt.ly/TwWv8qj3

I'm a Russian Occupant (2015). Retrieved from https://cutt.ly/dwWv3Nvg

Yavorska, H. (2018). The cognitive territory of hybrid warfare: a conflict of interests. *Strategic Communications in Hybrid Warfare: A Volunteer-to-Scientist View: A Monograph*. Kyiv: NA SB Ukrainy, 50-80 // **Яворська, Г.** (2018). Когнітивна територія гібридної війни: конфлікт інтересів. *Стратегічні комунікації в умовах гібридної війни: погляд від волонтера до науковця: монографія*. Київ: НА СБ України, 50-80.