

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ХАРЧЕНКО ІВАННА ОЛЕКСАНДРІВНА

Допускається до захисту:
в.о. завідувача кафедри
міжнародних відносин і зовнішньої
політики,
д.е.н., доцент
_____ В. В. Лимар
«_____» _____ 2024 р.

ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ В РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ

Спеціальність 291 Міжнародні відносини, суспільні комунікації та регіональні
студії

Кваліфікаційна (магістерська) робота

Керівник:
Паніна І. Г., к.і.н., старший викладач
кафедри міжнародних відносин і
зовнішньої політики

Оцінка: ____ / ____ / ____
(бали/за шкалою ECTS/за національною шкалою)

Голова ЕК:
Гижко А.П., д-р філософії за
спеціальністю 052 Політологія

(підпис)

Вінниця - 2024

АНОТАЦІЯ

Харченко І. О. Інформаційний тероризм в російсько-українській війні.

Спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії», освітня програма «Міжнародні комунікації та медіація в умовах конфліктного врегулювання». Донецький національний університет імені Василя Стуса, Вінниця, 2024.

У кваліфікаційній роботі узагальнено основи прояву інформаційного тероризму та засоби його реалізації в сучасному світі. Основна увага була приділена інформаційній терористичній діяльності РФ на тлі російсько-української війни. Здійснено спробу проаналізувати поняття «інформаційний тероризм», його особливості, чинники, способи реалізації та прослідкувати його активний розвиток на прикладі діяльності Росії як прихильника інформаційного терору.

Ключові слова: інформаційний тероризм, кібертероризм, ІПСО, пропаганда, Україна, російська федерація.

97 с., дод.4, 62 джерела.

Рис. 14. Бібліограф.: 100 найм.

ABSTRACT

Kharchenko I. O. Informational terrorism in the Russian-Ukrainian war.

Speciality 291 «International Relations, Public Communications and Regional Studies», study programme «International Communications and Mediation in the Conditions of Conflict Resolution». Vasyl' Stus Donetsk National University, Vinnytsia, 2024.

The qualification work summarizes the basics of the manifestation of information terrorism and the means of its implementation in the modern world. The main attention was paid to informational terrorist activities of the Russian Federation against the background of the Russian-Ukrainian war. An attempt was made to analyze the concept of "informational terrorism", its features, factors, methods of

implementation, and to follow its active development on the example of russia's activity as a supporter of informational terror.

Keywords: information terrorism, cyber terrorism, IPSO, propaganda, Ukraine, russian federation.

97 p., 4 appendix, 62 sources.

Fig. 14. Bibliography: 100 references.



ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	5
ВСТУП	6
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ	9
1.1 Поняття «інформаційний тероризм» і еволюція інформаційного тероризму як явища	10
1.2 Джерельна база та методологічна основа дослідження	18
РОЗДІЛ 2. ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ У СУЧАСНИХ ВІЙНАХ	25
2.1 Інформаційний тероризм як новий інструмент війни	26
2.2 Особливості взаємодії інформаційного тероризму з традиційними засобами ведення війни	33
2.3 Прояви державного інформаційного тероризму в конфліктах ХХІ ст.	37
РОЗДІЛ 3. ПРОЯВИ ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ У РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ	43
3.1 Вплив росії на український інформаційний простір в 1991-2022 роках	44
3.2 Кібервійна, пропаганда та психологічні операції рф після повномасштабного вторгнення	50
3.3 Боротьба України з російським інформаційним тероризмом в умовах війни	58
3.4 Вплив російського ІПСО на думку міжнародної спільноти щодо російсько-української війни	64
ВИСНОВКИ	70
СПИСОК ДЖЕРЕЛ І ЛІТЕРАТУРИ	74
ДОДАТКИ	87

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІПСО – інформаційно-психологічні операції

США – Сполучені Штати Америки

рф – російська федерація

ГУР – Головне управління розвідки

ЗСУ – Збройні Сили України

ЗМІ – засоби масової інформації

ЄС – Європейський Союз

РПЦ – російська православна церква

АЕС – атомна електростанція

МАГАТЕ – Міжнародне агентство з атомної енергії

ВСТУП

Актуальність теми дослідження. Інформаційний тероризм росії в Україні є важливою частиною сучасного глобального конфлікту, що відбувається на політичній та інформаційній аренах. російська федерація активно використовує інформаційні технології як інструмент маніпуляцій, психологічного тиску та дезінформації, що є ключовими складовими її агресивної зовнішньої політики. Під терміном “інформаційний тероризм” мається на увазі використання інформаційних засобів для досягнення стратегічних цілей через маніпулювання громадською думкою, викликання паніки, заплутування фактів, спотворення реальності та створення фальшивих наративів, які підтримують або виправдовують воєнні дії.

Феномен інформаційного тероризму росії має великий вплив на національну безпеку України, адже за допомогою дезінформації росія намагається створити “паралельну реальність”, яка би підривала моральний дух українського населення, заважала мобілізації та відновленню внутрішньої єдності, а також відволікала міжнародну підтримку України. Інформаційний тероризм дозволяє росії впливати на глобальну політичну ситуацію та формувати не лише внутрішній, а й зовнішній політичний ландшафт.

Вивчення інформаційного тероризму в контексті російсько-української війни є надзвичайно актуальним, оскільки ці методи можуть бути адаптовані й використані іншими державами у конфліктах, де інформаційний контроль є не менш важливим, ніж військова перевага. Розуміння механізмів інформаційного тероризму та розвиток ефективних контрзаходів є важливими для захисту національних інтересів та збереження демократії в умовах інформаційних війн. Саме тому важливим є формування критичного ставлення до інформації, що поширюється в умовах сучасної гібридної війни. Україні, а також всьому світу, необхідно уважно стежити за динамікою інформаційних війн, щоб мінімізувати їхні негативні наслідки та забезпечити стабільність у глобальному політичному середовищі.

Об'єктом дослідження є інформаційний тероризм як загроза міжнародній безпеці.

Предметом дослідження є основні характеристики та прояви інформаційного тероризму як інструмента російської агресії в Україні.

Мета роботи – визначити роль інформаційного тероризму в контексті російсько-української війни та виявити особливості реалізації терористичних дій в умовах війни за допомогою інформації.

Відповідно до мети було поставлено такі **завдання**:

- охарактеризувати поняття «інформаційний тероризм» і засоби його реалізації;
- визначити джерельну базу та методологічну основу дослідження;
- дослідити вплив інформаційного тероризму на перехід держав від традиційної форми ведення війни до гібридної;
- визначити можливості держав поєднувати інформаційний тероризм з традиційними засобами ведення війни;
- проаналізувати рівень зростання проявів державного інформаційного тероризму в конфліктах сучасності;
- дослідити вплив росії на інфопростір України з часів її незалежності та до повномасштабного вторгнення;
- порівняти терористичні прояви рф проти України напередодні та під час повномасштабної агресії в Україні;
- виявити потенційні та реальні загрози від інформаційного тероризму рф для інформаційної безпеки України;
- оцінити заходи України в сфері боротьби з російським інформаційним тероризмом в умовах;
- проаналізувати міжнародну реакцію на інформаційні атаки рф, її інформаційну політику та перспективи запровадження санкцій у зв'язку з інформаційним тероризмом.

Наукова новизна дослідження. Авторкою привернута увага до такого явища, як інформаційний тероризм, що не є популярною темою вітчизняних

досліджень. Було доповнено загальне розуміння державного тероризму через опис основних тактик і методів, використаних різними державами світу, для створення хаосу на певній території. Розширено перелік кейсів застосування інформаційного тероризму, в основному під час російсько-української війни.

Теоретичне та практичне значення отриманих результатів кваліфікаційної (магістерської) роботи полягає у аналізі інформаційного тероризму, як відносно нового явища, а також використання російською федерацією даного явища як одного з інструментів тероризму під час війни з Україною. Отримані результати дискусії про використання росією інформаційного тероризму у війні з Україною з теоретичного боку допомагають нам зрозуміти сутність, механізми та наслідки цього явища в контексті гібридної війни, а також можуть бути використані під час підготовки дотичних навчальних курсів і освітніх компонентів. У практичній площині вирішення цих питань має важливе значення для забезпечення національної безпеки, збереження демократичних інститутів та стабільності суспільства.

Апробація результатів дослідження. Результати дослідницьких розробок на тематику «Інформаційний тероризм в російсько-українській війні» були опубліковані у збірнику тез IV Міжнародної науково-практичної конференції Таврійського національного університету імені В. І. Вернадського у вигляді тез на тему: «Боротьба України з російським інформаційним тероризмом в умовах війни» (17-18 жовтня 2024 р.).

Структура роботи. Специфіка проблем, визначених предметом та об'єктом дослідження, його мета та завдання зумовили структуру роботи. Робота складається зі вступу, 3 змістовних розділів, 9 підрозділів, висновків, списку використаних джерел та літератури (100 найменувань) та додатків (14 рисунків). Загальний обсяг дослідження становить 97 сторінок, з яких 73 – основний текст.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ

Феномен інформаційного тероризму став критично важливою сферою в галузі досліджень безпеки, комунікації та міжнародних відносин. Він представляє новий вимір сучасної війни, де маніпулювання інформацією стає інструментом не лише для політичної чи військової переваги, але й для поширення страху, плутанини та психологічної дестабілізації. Теоретичні основи інформаційного тероризму спираються на політичну теорію, дослідження ЗМІ, психологію та вивчення війни і миру.

У цьому розділі досліджуються ключові теоретичні концепції та рамки, які формують наше розуміння інформаційного тероризму, зосереджуючись на його природі, механізмах і цілях, а також досліджуються теоретичні основи інформаційного тероризму, спираючись на основні дослідження як українських, так і міжнародних вчених. Розглядаються основні концепції, механізми та рамки, які дають зрозуміти, як маніпулюють інформацією для досягнення стратегічних політичних, військових і соціальних цілей. Теоретичні погляди, представлені в цьому розділі, є важливими для розуміння динаміки інформаційного тероризму та його впливу на глобальну безпеку.

Вічна дилема боротьби з тероризмом у демократичному суспільстві полягає в пошуку правильного балансу між громадянськими свободами та громадською безпекою. Швидкий розвиток інформаційних технологій, широке використання глобальних телекомунікаційних мереж і розвиток інформаційного суспільства створили нові загрози в цифровій сфері. Однією з істотних загроз є використання цих нових можливостей для терористичної діяльності, яка підриває життєво важливі інтереси окремих осіб, суспільства та держави. Як наслідок, ризик інформаційного тероризму в цифровому просторі стрімко зростає.

Вирішення питання боротьби з інформаційним тероризмом потребує глибокого аналізу еволюції самого тероризму, який пройшов шлях від окремих терористів-смертників до масштабних терористичних організацій, здатних організовувати руйнівні дії та спричиняти масові жертви. Такі організації використовують поширення інформації, щоб вселити страх не лише у населення конкретної держави, а і впливати на світову спільноту в цілому.

У сучасному суспільстві Інтернет ускладнив завдання захисту інформаційних ресурсів. Терористичні групи та окремі суб'єкти по всьому світу використовують його особливості та переваги, намагаючись впливати як на внутрішню, так і на зовнішню політику держав, використовуючи різні інформаційні технології для досягнення своїх злочинних цілей.

Таким чином, вивчення феномену інформаційного тероризму в контексті інформаційної безпеки є визначальним для національної безпеки. А також, надає в повному обсязі розуміння як з цим феноменом варто боротися та які заходи впроваджувати.

1.1 Поняття «інформаційний тероризм» і еволюція інформаційного тероризму як явища

Поява інформаційного тероризму обумовлена значною зміною природи конфліктів і війни в ХХІ столітті. Оскільки цифрова революція продовжує трансформувати суспільства, способи використання інформації як зброї стають все більш витонченими, що робить її одним із основних інструментів сучасної геополітичної та ідеологічної боротьби.

Інформаційний тероризм, як явище, можна розглядати як еволюцію традиційних тактик тероризму, але адаптованих до цифрової епохи. У минулому тероризм часто асоціювався з фізичним насильством, таким як вибухи або захоплення заручників. Однак сьогодні держави, недержавні організації та навіть окремі особи можуть використовувати Інтернет для здійснення кібератак, поширення фейкових новин і ведення психологічної війни. Ці тактики можуть

бути більш витонченими, але такими ж ефективними, часто спрямованими на психологічний стан цілого населення.

Існує багато дефініцій інформаційного тероризму, які перебувають переважно в юридичній площині. Найбільш вдалим є визначення, запропоноване В. Коршуновим: *інформаційний тероризм* – це новий вид терористичної діяльності, орієнтований на використання різних форм і методів тимчасового або незворотного виведення з ладу інформаційної інфраструктури держави або її елементів, а також за допомогою протиправного використання інформаційної структури для створення умов, що тягнуть за собою тяжкі наслідки для різних сторін життєдіяльності особистості, суспільства і держави [9, с.575].

Окремо можна виділити інформаційно-психологічний тероризм і його підвид – медіа-тероризм. На думку І. Коропа, *медіа-тероризм*, також відомий як “медіа-кілерство”, є використанням інформаційних систем, мереж та їх компонентів для проведення терористичних дій різного характеру. Сюди входить маніпуляція засобами масової інформації для поширення паніки, залякування населення або дестабілізації ситуації в суспільстві.

Інший вид пов'язаний із цією сферою – *інформаційно-технічний тероризм*, спрямований на завдання шкоди елементам інформаційного середовища або його повному функціонуванню. Це може включати дії, як-от штучне перевантаження комунікаційних вузлів, що призводить до порушення передачі даних і зв'язку між ключовими інфраструктурними об'єктами [18].

Обидва типи відображають тенденцію до використання технологій як інструменту для досягнення терористичних цілей, що є характерною рисою сучасної цифрової епохи.

Еволюцію інформаційного тероризму можна простежити ще до початку використання пропаганди під час світових війн. На думку авторки, його перетворення на особливу та потужну форму війни є відносно недавнім явищем, яке спричинене швидким розвитком цифрових медіа, соціальних мереж і технологічним прогресом. Розвиток інформаційного тероризму тісно

пов'язаний із розвитком цифрових засобів зв'язку та глобальним взаємозв'язком медіа-систем.

Витоки інформаційного тероризму можна простежити у I половині XX ст, коли пропаганда широко використовувалася під час Першої та Другої світових війн. Уряди та військові сили застосовували пропаганду, щоб вплинути на громадську думку, згуртувати підтримку військових зусиль і деморалізувати ворога. Одному з найвпливовіших дослідників цього питання, Е. Бернейсу [56], часто приписують закладення основ сучасних методів пропаганди. У своїй основоположній праці «Пропаганда» Бернейс стверджував, що пропаганда є важливим інструментом для формування громадської думки та управління демократичними суспільствами [56]. Хоча його робота була зосереджена на маркетингу та зв'язках з громадськістю, вона заклала основу для розуміння психологічних механізмів, які лежать в основі пропагандистських кампаній.

Під час Холодної війни інформаційно-психологічні операції (далі - ІПСО) стали невід'ємною частиною інформаційної війни, оскільки і Сполучені Штати, і Радянський Союз використовували ЗМІ та інформацію для ведення ідеологічних битв. У цьому контексті інформація стала інструментом маніпулювання суспільним сприйняттям, демонізації ворога та впливу на політичні рішення. Радянський Союз, зокрема, використовував широкі кампанії з дезінформації, щоб підірвати статус Заходу, тоді як уряд США використовував інформацію для просування своїх цінностей демократії та капіталізму.

Цифрова революція, що почалася наприкінці XX століття, кардинально змінила ландшафт інформаційної війни. Широке використання Інтернету, мобільних телефонів і платформ соціальних медіа дозволило інформації поширюватися швидше та охоплювати ширше відмінностей, ніж будь-коли раніше. Можливість маніпулювати громадською думкою через цифрові канали відкрила нові можливості для інформаційного тероризму. Як стверджує МакЧесні [85], швидкий розвиток цифрових комунікаційних платформ полегшив для акторів поширення дезінформації, маніпулювання суспільними настроями та дестабілізацію суспільства.

У 2000-х роках інформаційний тероризм став більш цілеспрямованим і стратегічним інструментом як у політичних, так і у військових конфліктах. «Помаранчева революція» 2004 року в Україні продемонструвала роль інформації у формуванні політичних результатів. Українські активісти та лідери опозиції використовували Інтернет і соціальні медіа для мобілізації протестів проти фальсифікованих президентських виборів, підкреслюючи потенціал цифрових медіа кинути виклик політичній владі. Однак це також створило основу для появи більш витончених форм маніпулювання інформацією, оскільки держави визнали силу інформації впливати на політичні події.

Однією з найважливіших віх в еволюції інформаційного тероризму стала окупація росією Криму в 2014 році та війна проти України.

Механізми інформаційного тероризму різноманітні та включають низку методів, призначених для маніпулювання, обману та дестабілізації. Ці механізми можна класифікувати за кількома категоріями: кампанії з дезінформації, інформаційно-психологічні операції, маніпуляції ЗМІ та кібератаки.

Дезінформація є основним інструментом інформаційного тероризму. Це передбачає навмисне поширення неправдивої або оманливої інформації з метою створення плутанини, навіювання страху та маніпулювання громадською думкою. Кампанії з дезінформації часто проводяться через цифрові платформи, включаючи соціальні мережі, веб-сайти та видання новин.

Президентські вибори в США 2016 року є яскравим прикладом того, як кампанії з дезінформації можуть бути використані для впливу на політичні результати. За даними Бенклера російські оперативники використовували соціальні медіа-платформи, такі як Facebook і Twitter, щоб поширювати розбіжний контент і впливати на громадську думку під час виборів [55]. Ці кампанії з дезінформації, які часто маскуються під масові рухи, були розроблені, щоб використовувати існуючі соціальні розбіжності та просувати конкретні політичні програми.

Ще одним ключовим механізмом інформаційного тероризму є *інформаційно-психологічні операції*. ІПСО передбачає використання психологічних маніпуляцій для впливу на ставлення, емоції та поведінку окремих осіб або груп. Ці операції можуть використовувати різноманітні інструменти, включаючи пропаганду, емоційні заклики та тактику страху.

Маніпуляція ЗМІ, як традиційними, так і цифровими, є потужним інструментом інформаційного тероризму. ЗМІ можна використовувати для поширення неправдивих наративів, формування громадської думки та виправдання дій. У контексті інформаційного тероризму маніпуляції засобами масової інформації часто включають контроль над потоком інформації для створення сприятливого наративу або делегітимізації опонентів. Це може включати використання контрольованих державою засобів масової інформації, вибіркове репортажі та посилення певних точок зору з одночасним замовчуванням інших.

Кібератаки все частіше використовуються в поєднанні з маніпуляціями ЗМІ, щоб порушити інформаційне середовище. Ці атаки можуть бути спрямовані на критичну інфраструктуру, викрасти конфіденційну інформацію або порушити канали зв'язку. Як стверджує МакЧесні [85], поєднання маніпуляцій ЗМІ та кібератак створює потужну зброю для дестабілізації урядів і суспільств, і авторка кваліфікаційної (магістерської) роботи з цим погоджується.

Інформаційний тероризм як концепція, описує навмисне та стратегічне використання інформаційно-комунікаційних технологій (ІКТ) для викликання збоїв, страху та нестабільності. У той час як тероризм традиційно відноситься до насильницьких дій, спрямованих на вселяння страху шляхом фізичної шкоди, інформаційний тероризм використовує інформацію як зброю для маніпулювання, обману та контролю суспільного сприйняття та поведінки.

Теоретичні основи інформаційного тероризму є мультидисциплінарними і охоплюють теорії комунікації, політології, психології та досліджень безпеки. Для розуміння того, як інформація стає зброєю та як вона впливає на окремих осіб, групи та суспільства в цілому, було розроблено кілька ключових основ.

Найбільш актуальними теоріями для вивчення інформаційного тероризму є теорія фреймінгу, теорія пропаганди, дослідження інформаційно-психологічних операцій (ІПСО) та теорія мереж. Ці рамки допомагають пояснити, як функціонує інформаційний тероризм та його наслідки для сучасних суспільств.

Теорія фреймінгу, представлена Р. Ентманом [65], надає корисну лінзу для розуміння того, як конструюється та подається інформація, щоб впливати на сприйняття громадськості. Основна передумова теорії фреймінгу полягає в тому, що інформація не є нейтральною, а вибірково формується її виробниками, щоб висвітлити певні аспекти проблеми та применшити інші. У контексті інформаційного тероризму теорія фреймінгу допомагає пояснити, як злочинці маніпулюють наративами для досягнення конкретних цілей.

Теорія фреймінгу також припускає, що інформаційний тероризм діє через вибіркове представлення фактів, емоційні заклики та візуальні образи, які спотворюють суспільне сприйняття. Формуючи наратив, інформаційні терористи можуть впливати на те, як люди інтерпретують події, роблячи фреймінг ключовим інструментом в арсеналі інформаційної війни.

Модель пропаганди Е. Германа та Н. Хомського, представлена в їхній книзі “Manufacturing consent: The political economy of the mass media” [70], стверджує, що засоби масової інформації часто використовуються впливовою елітою для контролю та маніпулювання громадської думки. З цієї точки зору, ЗМІ, особливо в демократичних суспільствах, структуровані таким чином, щоб служити інтересам державних і корпоративних акторів. Ці еліти формують інформаційне середовище через контроль над медіа-каналами, формулюючи завдання для збереження політичної та економічної влади.

У контексті інформаційного тероризму теорія пропаганди є особливо актуальною, якщо розглядати, як державні та недержавні актори маніпулюють громадською думкою через ЗМІ. Інформаційний тероризм використовує інструменти пропаганди, щоб контролювати потік інформації, використовуючи як традиційні медіа (телебачення, радіо, друковані видання), так і нові медіа

(соціальні мережі, веб-сайти) для поширення повідомлень, які підтримують конкретні плани.

Пропагандисти, як у мирний, так і в воєнний час, використовують *інструменти для маніпулювання думками*. Важливими інструментами є стимулювання, навіювання, натяки, апеляція до бажань.

Одним із таких методів є пропозиція або стимулювання. Пропагандист прагне змусити людей приймати його твердження без сумнівів або діяти відповідно до його бажань. Для цього часто використовується навіювання, що допомагає уникнути критики і змусити аудиторію прийняти пропозицію без логічних підстав. Наприклад, нацистська пропаганда використовувала твердження про зраду євреїв під час Першої світової війни. Ще один метод – це звернення до бажань аудиторії. Пропагандисти вивчають громадську думку, щоб використовувати слова, що викликають позитивні чи негативні асоціації, залежно від своїх цілей. Наприклад, Гітлер використовував цю техніку, звертаючись до різних груп у Німеччині, пропонуючи вирішення їхніх проблем.

Інформаційно-психологічні операції (ІПСО) стосуються використання психологічних технік для впливу на сприйняття, ставлення та поведінку окремих осіб або груп з метою досягнення стратегічних цілей. ІПСО були невід'ємною частиною військової стратегії протягом десятиліть, і їх застосування до інформаційного тероризму має вирішальне значення для розуміння того, як інформація використовується як зброя. Вони покладаються на емоційні маніпуляції, тактику страху та дезінформацію, щоб дестабілізувати цільові групи населення, порушити соціальну згуртованість і деморалізувати опонентів.

Теорія мереж, яка досліджує потік інформації через взаємопов'язані системи, є ще однією ключовою основою для розуміння інформаційного тероризму. Згідно з теорією мереж, інформація протікає через соціальні мережі за закономірностями, на які може впливати структура та зв'язок мережі.

Одним із найважливіших аспектів теорії мереж у контексті інформаційного тероризму є здатність інформації швидко поширюватися через

соціальні медіа. Такі дослідники, як Й. Бенклер [55], стверджують, що децентралізований характер цифрових мереж полегшує інформаційним терористам швидке поширення своїх повідомлень у великих географічних зонах. Вірусний характер контенту на платформах соціальних мереж у поєднанні з використанням ботів і фейкових облікових записів дозволяє інформаційним терористам створити відчуття консенсусу навколо неправдивого або оманливого наративу.

Концепція інформаційного тероризму та його еволюція як явища відображають зростання значення інформації в сучасних конфліктах. Оскільки цифрові технології продовжують розвиватися, інформаційний тероризм залишатиметься ключовим інструментом як для державних, так і для недержавних акторів, які прагнуть маніпулювати громадською думкою, дестабілізувати суспільства та досягати стратегічних цілей.

Аналізуючи історичний розвиток і механізми інформаційного тероризму, ми можемо краще зрозуміти його наслідки для глобальної безпеки та майбутнього війни, а розуміння теоретичних перспектив, дає змогу розібратися з динамікою інформаційного тероризму та його впливом на глобальну безпеку. Оскільки цифрові технології продовжують розвиватися, роль інформації як інструменту ведення війни буде тільки зростати, що робить вивчення інформаційного тероризму все більш важливим для дослідників, політиків і практиків.

Проблема розвитку та поширення *державного інформаційного тероризму* є доволі популярною темою у сучасних міжнародно-політичних дослідженнях. Усі роботи, представлені українськими та зарубіжними авторами, умовно можна поділити на кілька категорій:

- загальні праці, присвячені проблемі інформаційного тероризму (Е.Бернейс, Р. МакЧесні та ін.);
- дослідження інформаційного тероризму, як інструмента сучасних війн (роботи М. Лібікі, Ф. Г. Хоффмана та ін.);

- окрему групу становлять праці, присвячені питанню державного інформаційного тероризму рф під час війни з Україною (роботи К. Герасименко, В. Коршунов, Б. Леонов, Г. Лисько, С. Лихової).

Незважаючи на великий масив наукових доробок, значно менше уваги дослідників приділено сучасному поєднанню інформаційного тероризму та традиційних методів ведення війни, яке використовує росія в умовах війни з Україною, що актуалізує тему кваліфікаційної (магістерської) роботи.

1.2 Джерельна база та методологічна основа дослідження

Дослідження інформаційного тероризму вимагає комплексного підходу, що поєднує кілька методологічних підходів. У цьому дослідженні прийнято *концепцію секторальної безпеки*, розроблену Б. Бьюзеном, яка розглядає безпеку як багатовимірну структуру, що охоплює політичний, військовий, соціальний, економічний та екологічний сектори [61]. Застосовуючи цю структуру, інформаційний тероризм аналізується як загроза сектору інформаційної безпеки України, взаємопов'язана з політичним і суспільним вимірами. Цей підхід дає змогу детально зрозуміти, як кампанії з дезінформації дестабілізують демократичні процеси, поляризують суспільства та підривають суверенітет держави.

Системний підхід лежить в основі дослідження, концептуалізуючи інформаційний тероризм як інтегровану систему, що включає акторів, інструменти та результати. Ця структура дозволяє розділити явище на такі компоненти, як державні та недержавні суб'єкти (наприклад, російські державні установи та афілійовані медіа), інструменти (наприклад, пропаганда, маніпуляції в соціальних мережах) і наслідки (наприклад, ерозія довіри до уряду). установи). Таким чином, системна перспектива забезпечує цілісний аналіз взаємопов'язаних елементів інформаційного тероризму.

Системний підхід дозволяє розглянути інформаційний тероризм як багатопланове явище, що діє в різних сферах. Цей принцип гарантує, що під час

аналізу враховуються не лише прямі наслідки кампаній з дезінформації, але й їхній вплив на соціальну згуртованість, політичну стабільність і національну безпеку. Наприклад, системний підхід допоміг у картографуванні того, як наративи російської пропаганди вплинули на громадську думку на окупованих територіях.

Міждисциплінарний підхід ще більше посилює дослідження, синтезуючи ідеї з таких галузей, як міжнародні відносини, медіадослідження, кібербезпека та психологія. Ця міждисциплінарна інтеграція дозволяє дослідженням охопити технічні, комунікативні та психологічні виміри інформаційного тероризму, пропонуючи повне розуміння його механізмів і наслідків.

Міждисциплінарний підхід сприяє інтеграції різноманітних академічних і практичних перспектив, забезпечуючи багатогранний аналіз інформаційного тероризму. Завдяки поєднанню методологій кібербезпеки (наприклад, цифрової криміналістики), медіа-досліджень (наприклад, аналіз контенту) та психології (наприклад, вивчення страху як інструменту пропаганди), цей принцип дозволив визначити інноваційні стратегії протидії інформаційному тероризму.

Описані вище методологічні підходи були реалізовані в кваліфікаційному (магістерському) дослідженні шляхом залучення широкого кола джерел у таких сферах, як кібербезпека, медіааналіз, міжнародні відносини та безпека.

За походженням джерела умовно можна поділити на шість груп:

- 1) міжнародно-правові акти і документи міжнародних організацій;
- 2) законодавчі акти України;
- 3) документи органів державної влади;
- 4) матеріали медіа;
- 5) матеріали соціальних мереж;
- 6) довідкова література.

Перша група джерел представлена міжнародно-правовими актами, серед яких чільне місце посідають конвенції, міжнародні протоколи та документи міжнародних організацій:

- Конвенція ООН “Про заборону застосування, накопичення запасів, виробництва і передачі протипіхотних мін та про їхнє знищення” від 18.09.1997 р. [14];

- Конвенція ООН “Про захист цивільного населення під час війни” від 12.08.1949 р. [15];

- Протокол ООН “Про вибухонебезпечні предмети - наслідки війни” від 28.11.2003 р. [34];

- II Гаазька конвенція 1907 р. [68];

- Варшавське комюніке саміту НАТО 2006 р. [98].

Дані акти були використані в дослідженні для визначення міжнародних стандартів і правових рамок, що регулюють поведінку під час збройних конфліктів, включно з протидією інформаційному тероризму. Ці документи забезпечили розуміння зобов’язань держав-учасниць у сфері захисту цивільного населення, знищення засобів терору, а також зменшення наслідків війни для постраждалих територій. Аналіз цих актів дозволив простежити, як міжнародно-правові норми можуть слугувати основою для розробки національних стратегій протидії гібридним загрозам і збройній агресії.

Законодавчі акти України - *друга група джерел* цього магістерського дослідження. Такі закони України, як Закон України «Про внесення змін до деяких законодавчих актів України щодо заборони політичних партій» (03.05.2022 р. № 2243-IX) [29], Закон України «Про забезпечення функціонування української мови як державної» (25.04.2019 р. № 2704-VIII) [30], Закон України «Про захист конституційного ладу у сфері діяльності релігійних організацій» (20.08.2024 р. № 3894-IX) [31], а також рішення Ради національної безпеки і оборони України «Про створення Центру протидії дезінформації» (11.03.2021 р.) [32], дають розуміння правових механізмів, які Україна застосовує для протидії інформаційному тероризму, захисту державного суверенітету, конституційного ладу та національної ідентичності.

Перелічені законодавчі акти допомогли виявити роль законодавства у формуванні стратегій захисту від російської агресії, особливо в інформаційній

сфері, через заборону проросійських політичних сил, захист української мови як ключового елемента національної ідентичності, обмеження діяльності деструктивних релігійних організацій та централізовану боротьбу з дезінформацією.

Третя група джерел не є чисельною і представлена документами органів державної влади, які зосереджені в основному на офіційному сайті Міністерства культури та стратегічних комунікацій (до 6.09.2024 - Міністерство культури та інформаційної політики) [24]. Урядові звіти, включаючи аналізи Міністерства інформаційної політики України та Центру стратегічних комунікацій при зазначеному міністерстві [36], надають емпіричні докази російських інформаційних операцій.

Четверта група джерел є найбільшою за кількістю матеріалів, адже це публікації в ЗМІ. Медіаконтент таких платформ, як RT і Sputnik, було проаналізовано, щоб зрозуміти наративи, які поширюють російські державні ЗМІ. Під час написання магістерської роботи було проаналізовано матеріали таких закордонних медіа як: The Economist, Variety, RAND, The New York Times, NPR, OC Media, The Defence Horizon Journal, а також українських - Explainer, LB.ua. АрміяInform, VoxUkraine, BBC News Україна, ГЛАВКОМ, Детектор медіа, Слово і діло, Укрінформ, Радіо Свобода, Економічна правда, Chas News, Суспільне Київ, Ukraïner.

Матеріали ЗМІ були використані для аналізу інформаційних наративів, маніпулятивних практик і стратегії впливу на аудиторію в контексті інформаційного тероризму. Аналітичні публікації та репортажі із закордонних видань допомогли оцінити масштаби поширення російської пропаганди, її вплив на політичні процеси в інших країнах та спроможність демократичних суспільств протидіяти гібридним загрозам. На противагу українські медіа відіграли ключову роль у висвітленні реального стану інформаційного протистояння між Україною та росією. Ці джерела надали емпіричні дані про вплив дезінформаційних кампаній на українське суспільство, а також показали, як українські медіа працюють у кризових умовах, протидіючи пропаганді.

Матеріали соціальних мереж, в тому числі ті, які містять приклади інформаційних атак, становлять *п'яту групу джерел*. Дані з соціальних мереж, особливо Telegram, включаючи метадані та журнали активності, використовувалися для виявлення моделей і стратегій у онлайн-кампаніях дезінформації. Крім того, візуальний матеріал кваліфікаційної роботи було взято саме з соціальних мереж (додаток Г).

Довідкова література (*шоста група джерел*) дозволяє наповнити магістерське дослідження кількісними даними. Наприклад, авторка звернулася до платформи Global Conflict Tracker [62] щоб отримати кількісні дані, для порівняння інформаційного тероризму Росії в Україні з аналогічними випадками у світовій практиці, що дозволяє визначити специфіку цього явища в українському контексті. Крім того, платформа дозволила вивчити кількісні показники впливу дезінформації, зокрема, зміну суспільної думки, соціальні наслідки та рівень довіри до офіційних джерел інформації.

Отже, використання різноманітних джерел дозволило провести дослідження із залученням цікавих кейсів і сприяло формуванню авторкою самостійних висновків, що було б неможливо без певних методологічних прийомів.

Основу кваліфікаційної роботи становлять загальнонаукові (аналітико-синтетичний, індуктивно-дедуктивний) та спеціальні методи дослідження (контент-аналіз, психолінгвістичний аналіз, мережевий аналіз).

Метод аналізу був вирішальним для розкладання явища інформаційного тероризму на складові частини. Вивчаючи конкретні приклади, такі як поширення неправдивих наративів під час окупації Криму в 2014 році [100], цей метод допоміг визначити ключових акторів, стратегії та цільову аудиторію. Аналіз дозволив класифікувати методи пропаганди, такі як використання закликів до страху або звернення до ідентичності.

Метод синтезу, своєю чергою, використовувався для інтеграції висновків різних джерел і створити цілісну картину того, як діє інформаційний тероризм. Наприклад, поєднання медіа-аналізу з журналами активності в соціальних

мережах показало, як російські кампанії координуються між платформами, щоб розширити свої наративи.

Індукція сприяла виведенню ширших моделей із конкретних випадків кампаній дезінформації. Наприклад, неодноразове використання тактики делегітимізації в російських наративах призвело до висновку, що підриг довіри до демократичних інституцій є центральною метою їхніх інформаційних операцій.

Дедукція використовувалася для перевірки гіпотез, виведених з теоретичних основ. Наприклад, гіпотеза про те, що інформаційний тероризм використовує емоційно насичену мову для маніпулювання аудиторією, була перевірена за допомогою аналізу російських ЗМІ. Отримані дані підтвердили, що в таких матеріалах переважають слова, які викликають страх, гнів і розкол.

Контент-аналіз використовувався для вивчення наративів і стратегій обміну повідомленнями в російських медіа та публікаціях у соціальних мережах. Цей метод виявив повторювані теми, такі як зображення України як держави, що не вдалася, або НАТО як агресора. Визначивши частоту та охоплення цих наративів, контент-аналіз надав емпіричні докази системного підходу росії до інформаційної війни.

Мережевий аналіз, або аналіз мережі допоміг у вивченні структури та динаміки онлайн-кампаній дезінформації. Шляхом відображення взаємодії між обліковими записами соціальних мереж, які беруть участь у поширенні пропаганди, цей метод визначив центральні вузли (наприклад, впливові облікові записи або боти), які керують процесом поширення. Аналіз мережі також виявив роль автоматизованих облікових записів у поширенні дезінформації.

Психолінгвістичний аналіз використовувався для оцінки емоційного та психологічного впливу пропагандистських повідомлень. Цей метод був зосереджений на виявленні мовних шаблонів, які викликають страх, гнів або розкол, наприклад, емоційно заряджених прикметників або апокаліптичних рамок. Наприклад, російські ЗМІ часто використовували такі терміни, як «геноцид» або «фашизм», щоб маніпулювати сприйняттям України.

Підводячи підсумки до розділу 1, зауважимо, що джерельна та методологічна база цього дослідження є міцним підґрунтям для аналізу інформаційного тероризму в контексті російсько-української війни. Завдяки інтеграції теорії секторальної безпеки, системних і міждисциплінарних принципів, а також ряду загальнонаукових і спеціальних методів дослідження досягає всебічного розуміння цього складного явища. Отримані дані не лише висвітлюють стратегії та наслідки російського інформаційного тероризму, але й пропонують практичні ідеї для розробки контрзаходів для захисту інформаційної безпеки України.

РОЗДІЛ 2

ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ У СУЧАСНИХ ВІЙНАХ

Еволюція воєнних дій у ХХІ столітті змінила ландшафт глобальних конфліктів, а інформація стала основною зброєю. Інформаційний тероризм, підвид психологічної та інформаційної війни, призначений для маніпулювання громадською думкою, дестабілізації урядів і підриву довіри до інституцій. У цьому розділі досліджується роль інформаційного тероризму в сучасній війні та його інтеграція в гібридну війну, розглядається взаємодія між кіберопераціями, пропагандою та звичайними військовими стратегіями. Ключові дослідники в цій галузі, зокрема Френк Г. Хоффман та інші, сформуvalи концептуальну основу гібридної війни, підкреслюючи критичну роль маніпулювання інформацією.

Вплив інформаційної війни, зокрема в контексті соціальних мереж, став визначальною стратегією сучасної війни. Інформаційна війна використовує взаємозв'язки та безпосередність, яку забезпечують платформи соціальних мереж, щоб поширювати дезінформацію, маніпулювати наративами та сіяти розбрат між цільовими групами. Його тактика може формувати громадську думку, впливати на політичні процеси та дестабілізувати цілі національні держави, підриваючи довіру до інститутів і демократичних процесів. Нормалізація дезінформації та використання існуючих соціальних платформ посилюють силу таких кампаній з дезінформації.

У сучасну епоху соціальних медіа державні актори використовують цифрову пропаганду та маніпуляції, щоб формувати наративи, а також сприяти розбрату, щоб просувати свої геополітичні плани. За визначенням В.О'Донелла і Дж.Говета, ця форма пропаганди є прорахованим і скоординованим процесом, призначеним для поширення та розширення оманливого вмісту на багатьох платформах соціальних медіа [87].

2.1 Інформаційний тероризм як новий інструмент війни

Інформаційний тероризм виходить за межі локальних конфліктів, стаючи глобальним інструментом маніпулювання суспільним сприйняттям і дестабілізації націй без прямого військового втручання. Його адаптивність до сучасної гібридної війни дозволяє як державним, так і недержавним акторам використовувати вразливі місця у відкритих суспільствах, перетворюючи доступність інформації на зброю. Історично пропаганда поширювалася через пресу, радіо та телебачення з чітким авторством і обмеженим охопленням, однак цифрова революція розширила масштаби та швидкість дезінформації.

В останні десятиліття *інформаційний тероризм став потужним інструментом у гібридній війні*, що дозволяє державним та недержавним суб'єктам використовувати вразливості в системах цифрових комунікацій для впливу на населення та порушення управління. На відміну від традиційних актів насильства, інформаційний тероризм використовує дезінформацію та психологічні маніпуляції як його основну зброю. Ці методи спрямовані на досягнення стратегічних цілей, таких як підрив довіри до інститутів, посіву розбрату в суспільствах та вплив на політичні результати.

Сучасні військові конфлікти становлять серйозну загрозу для міжнародної спільноти через свій гібридний характер, що поєднує традиційні збройні дії з нетрадиційними методами, такими як інформаційні операції. У жовтні 1998 року Міністерство оборони США представило «Спільну доктрину інформаційних операцій» [94], яка визначила принципи розробки концепцій інформаційної війни та безпеки, а також уточнила ключові терміни для забезпечення єдності підходів і злагодженості дій Збройних Сил на всіх рівнях. Інформаційні операції (атаки) в цьому документі описані як «дії, спрямовані на ускладнення збору, обробки та зберігання інформації» [94]. Наслідком таких атак є спотворення суспільної свідомості через шкідливу інформацію, що змінює цінності та інтереси людей, підриває суверенітет держави і порушує її територіальну цілісність.

Концепція гібридної війни не є новою. Вона поєднує традиційну війну з нетрадиційними та нерегулярними військовими діями, зосереджуючись на великих масштабах наслідків, досяжних за допомогою помірних засобів, таких як перешкоджання військовим операціям противника або запобігання політичній підтримці населення. Гібридні конфлікти зазвичай застосовують більш м'які тактики, використовуючи більш комплексну стратегію, яка змінюється в інтенсивності через різні етапи - ініціацію, ескалацію та розв'язання, спрямовані на дестабілізацію внутрішніх і зовнішніх процесів держави [22].

Основною метою є підриз цільової держави через стимулювання економічної дестабілізації, розчарування та невдоволення населення, розколу серед меншин чи постраждалих груп, сприяння контрольованих та неконтрольованих міграції, придушення громадянського опору та порушення критичної інфраструктури. Це досягається через вибіркове використання розвідувальних операцій, місії сил спеціального призначення, звичайні військові дії та нерегулярних бійців (терористів, злочинців, ополченців, найманців, рухи опору, партизан тощо).

Використання інформації як зброї у війні вивчалось кількома вченими та дослідниками, які намагалися визначити та класифікувати різноманітні техніки та стратегії. Однією з найвпливовіших фігур у цій галузі є Френк Г. Хоффман, який представив концепцію гібридної війни. Хоффман стверджує, що гібридна війна передбачає інтеграцію звичайних військових тактик із нерегулярними методами, такими як кібератаки, дезінформація та інші форми некінетичної агресії [73]. Таке поєднання традиційних і нетрадиційних тактик стало характерною рисою сучасного державного управління, коли державні суб'єкти все більше покладаються на інформаційний тероризм для досягнення своїх цілей.

Іншим важливим вченим у галузі інформаційних війн є Мартін С. Лібікі, який досліджує стратегічні наслідки кібервійни та маніпулювання інформацією. Робота Лібікі підкреслює роль інформаційних систем у сучасних конфліктах,

стверджуючи, що контроль над інформаційними мережами став таким же важливим, як контроль над фізичною територією. Його аналіз кібератак як інструменту спонсорованого державою тероризму допоміг зрозуміти роль технологій у сучасній війні [82].

У 1995 році Національний інститут оборони США опублікував роботу М.Лібікі «Що таке інформаційні воєнні дії?» [95], у якій були визначені основні характеристики інформаційної зброї як частини інформаційної атаки або операції. Серед основних елементів інформаційної зброї зазначені :

- розповсюдження розвідувальної інформації;
- дезінформація;
- психологічні операції;
- фізичне знищення інформаційних ресурсів ворога;
- атаки (як фізичні, так і електронні) на інформаційну інфраструктуру противника;
- зараження комп'ютерних мереж вірусами та несанкціоноване проникнення в інформаційні мережі [95].

Однією з визначальних особливостей гібридної війни є складність розрізнення між мирним і військовим часом. Інформаційний тероризм сприяє цій неоднозначності, підтримуючи постійний стан психологічного конфлікту.

Сучасний приклад гібридної війни можна чітко проілюструвати поточними подіями в Україні, де бої виходять за межі фізичного поля бою і охоплюють економічну, дипломатичну, інформаційну (включаючи психологічну, кібернетичну та дезінформаційну) та політичну війну. Український науковець Є.Магда досить повно проаналізував російську гібридну стратегію впливу в Україні за весь період відновлення незалежності, приділивши значно більше уваги подіям російсько-української війни [22]. Концепція в основному базується на здатності націлюватися на віддалені об'єкти та процеси за допомогою нетрадиційних військових засобів, особливо критичних для військових функцій держави.

Інформаційний та технологічний розвиток надав можливість державам вирішувати конфлікти не військовими методами, а інформаційними. Перші несуть великі кількості людських втрат, а другі спрямовані на зміну психологічного настрою в суспільстві, наслідки яких ще надовго закарбовуються в історичній пам'яті людей, та впливають на їх життя протягом століть.

Інформація, як універсальний і дешевий інструмент, має необмежений радіус дії та надзвичайно високу ефективність, що може робити її більш небезпечною, ніж традиційні методи ведення війни. На перший погляд, вона не спричиняє фізичних руйнувань, які зазвичай супроводжують збройні конфлікти. Проте її вплив проявляється у здатності атакуючої сторони підривати інституційні основи та фундаментальні цінності противника, створювати хаос і перешкоджати поширенню правдивої інформації. Використовуючи психологічну маніпуляцію громадською думкою, інформаційна війна встановлює межу між реальністю та вигадкою, досягаючи стратегічних цілей без застосування фізичної сили.

Усвідомлення розвитку науково-технічної сфери, який створив умови для впровадження нових технологій, які не завжди спрямовані на благо суспільства, спонукало ключових гравців сучасних міжнародних відносин визнати кібер- та гібридні загрози головними викликами для держав-членів, що було офіційно закріплено на Варшавському саміті НАТО у 2016 році [98].

Попри те, що сучасні технології є одним із найбільших досягнень цивілізованого світу, не можна ігнорувати проблеми, які супроводжують технічний прогрес. За останні десять років масштаби поширення дезінформації через Інтернет стрімко зросли. Разом із цим спостерігається активізація пропаганди, шпигунства, неконтрольованого витоку державної таємниці й персональної інформації, а також масштабних кібератак.

Кібератаки є ще одним ключовим проявом спонсорованого державою інформаційного тероризму. Ці атаки спрямовані на критичну інфраструктуру, таку як електромережі, фінансові системи та мережі зв'язку, з метою порушити

функціонування держави чи суспільства. Кібератаки можуть використовуватися для викрадення конфіденційної інформації, вимкнення ключових служб або завдання економічної шкоди, що сприяє дестабілізації цільової держави.

Один із прикладів кібератак, спонсорованих державою, стався у 2007 році, коли росія здійснила серію кібератак проти Естонії. Вважається, що атаки, спрямовані на урядові веб-сайти, банківські системи та засоби масової інформації, стали відповіддю на демонтування радянських символів у Нарві. Кібератаки на кілька днів зруйнували естонське суспільство, паралізувавши цифрову інфраструктуру країни та продемонструвавши вразливість сучасних держав до кібервійни. Атаки також підкреслили зростаючу роль інформаційного тероризму в державному управлінні, оскільки порушення роботи інформаційних систем і комунікаційних мереж може мати глибокий психологічний і політичний вплив на цільове суспільство.

Крім того, інформаційний тероризм, який спонсорує держава, може мати довгострокові наслідки для глобальної безпеки. Зростаюча залежність від цифрових технологій та Інтернету зробила інформаційні системи все більш вразливими до кібератак і кампаній з дезінформації. Це, у свою чергу, створило нові можливості для державних акторів брати участь у таємних операціях, які підривають стабільність конкуруючих держав і кидають виклик домінуванню встановленої влади. Активність в цьому напрямку не важко помітити серед великих держав, котрі борються за домінування на світовій арені. Кожна з них використовує різні методи для досягнення своїх цілей.

З розвитком Інтернету, збором даних та посиленням конкуренції серед великих держав деякі країни, зокрема Китай, використовують його для контролю над своїми громадянами та поширюють цифровий авторитаризм по всьому світу. Окрім того, Росія та Китай ведуть інформаційну війну з Заходом, аби здобути перевагу та вплинути на західне суспільство. У цьому контексті зростає співпраця та координація між Китаєм і росією під керівництвом Сі Цзіньпіна та володимира путіна в галузях військової, геоекономічної,

геополітичної та стратегічної важливості, що ставить під сумнів глобальний порядок, який існує на Заході [52].

Китай і Росія, як авторитарні режими, продемонстрували готовність і здатність координувати інформаційні війни на рівні всього уряду. Ці держави володіють інструментами для проведення цілеспрямованих інформаційних кампаній, спрямованих на досягнення цілей, які суперечать міжнародним нормам і стандартам відповідальної поведінки у XXI столітті. Західний світ опинився у невідгданому становищі в цій сфері та має підстави для хвилювання, оскільки росія та Китай активно обмінюються досвідом, щоб ефективніше протидіяти західному впливу у своїх регіонах.

В сучасному світі не лише держави прагнуть світового панування та збільшення своєї ролі на міжнародній арені. До використання інформаційного тероризму вдаються і терористичні угруповання які, ведуть боротьбу з державами світу за право існування власної ідеології та створення власної держави. Завдяки своїй, так би мовити, «співпраці» з телеканалами, соціальними мережами та доступом до мережі Інтернет, терористи з кожним днем все більше збільшують свій вплив на населення. Маніпуляції з боку терористів все частіше зустрічаються на інформаційних платформах. Завдяки такій діяльності вони з легкістю можуть насаджувати людям свою ідеологію, свої бачення та навіть висвітлювати себе та свою діяльність як в нейтральному так і в позитивному сенсі. Також, це чудовий спосіб для вербування людей та збільшення прихильників їхньої діяльності, а також приєднання людей до рядів терористів.

До прикладу, Аль-Каїда на Аравійському півострові (AQAP) використовує соціальні медіа та онлайн-пропаганду вже більше десяти років, зокрема запустила свій англomовний цифровий журнал у 2010 році, який вплинув на теракти під час Бостонського марафону [77]. Талібан також стратегічно використовує соціальні мережі, керуючи своїм Telegram-каналом «al-Emarah», а також каналами пушту, перською та турецькою мовами. Зображення Талібаном своїх керівних можливостей у його пропаганді відіграло ключову роль у

залученні бойовиків і позиціонуванні себе як легітимної керівної сили, що відрізняє його від більшості інших агресивних екстремістських груп.

Інформаційна війна може доповнювати традиційні бойові операції, впливаючи як на стратегії на полі бою, так і на громадську думку. Отже, сучасна війна має чотири виміри: військовий, економічний, політичний і пропагандистський, що разом становлять комплексний тиск на супротивника. У двадцятому столітті було зрозуміло, що лише використання сили недостатньо для досягнення остаточної і тривалої перемоги. Війна ведеться на всіх чотирьох фронтах одночасно.

Розглядаючи пропаганду, як один із методів інформаційного тероризму, який взаємодіє з традиційними методами ведення війни, її використання під час збройного зіткнення має на меті деморалізувати супротивника, послаблюючи його моральний дух. Головна мета такої пропаганди — зламати бажання ворога боротися. Це досягається різними способами, зокрема через демонстрацію військових досягнень, уявлення про економічну та військову силу, з якою ворог повинен стикатися, а також через показ моральної переваги справи, проти якої ведеться боротьба [56].

Приклад того, як працює пропаганда в умовах війни, чітко прослідковується в умовах російсько-української війни після повномасштабного вторгнення. Постійні ракетні обстріли по цивільному населенню та по критичній інфраструктурі разом з використанням пропаганди щодо керівництва держави, великою мірою впливає на моральний настрій в суспільстві.

Варто зазначити, що пропаганда використовується не лише для деморалізації цивільних, а також і для поширення негативних настроїв серед військових. Таку тактику використовувала росія здебільшого на початку повномасштабного вторгнення шляхом поширення інформації про насильницьку діяльність збройних сил рф на окупованих територіях. Жахливі новини про гвалтування жінок, та вбивства дітей психологічно впливали на стан українських військових, адже головна їхня причина знаходження на фронті, це

захист цивільного населення. Таким чином, можна стверджувати, що інформаційна війна може впливати на хід воєнних дій.

Співіснування в одній площині методів інформаційного тероризму та традиційних засобів ведення війни є наразі популярним поєднанням. Війна в своєму звичному стані відходить на другий план, а в поєднанні з інформаційними можливостями набуває зовсім іншого значення та бачення. На думку авторки, навряд колись інформаційна війна повністю замінить традиційну війну, скоріш за все вона перетвориться на ще один засіб в умовах боротьби держав за свої геополітичні, економічні чи географічні цілі, адже слово не вбиває - вбиває зброя.

2.2 Особливості взаємодії інформаційного тероризму з традиційними засобами ведення війни

Загалом, міжнародне гуманітарне право забороняє засоби та методи, які спричиняють зайві ушкодження або непотрібні страждання. У результаті певні типи зброї заборонені, а спосіб використання іншої зброї обмежений. Основними договорами, що обмежують методи і засоби ведення війни, є Гаазька конвенція 1907 року [68], Додаткові протоколи 1977 року [15] до Женевських конвенцій і низка угод щодо конкретних видів зброї. Конкретні заходи щодо обмеження використання певних типів зброї включають також Оттавську конвенцію про заборону протипіхотних мін 1997 року [14], Протокол про вибухонебезпечні пережитки війни 2003 року (доповнення до Конвенції ООН про певні види звичайної зброї 1980 року) [34].

Вибір розпочати класичну війну зазвичай передбачає значні економічні та політичні витрати, які переважно несе громадянське суспільство. Ці особливості війни були радикально змінені з появою інформаційного тероризму, який надає засоби для ведення війни зовсім іншим способом. У цьому сценарії зміни, визначені інформаційним тероризмом, мають вражаюче значення, оскільки вони стосуються того, як військові та політики бачать ведення війни,

так і того, як війна сприймається громадянським суспільством. Як і традиційна війна, інформаційний тероризм є дуже потужним і потенційно дуже руйнівним. Однак, на відміну від традиційної війни, він є потенційно без людських втрат, економічно ефективним і не є специфічним військовим явищем.

Взаємодія між інформаційним тероризмом і традиційними засобами ведення війни стала визначальною рисою сучасних конфліктів, суттєво змінюючи спосіб ведення та сприйняття воєн. Ця взаємодія особливо очевидна в контексті гібридної війни, де звичайні військові операції поєднуються з некінетичними стратегіями для досягнення політичних і стратегічних цілей. Інформаційний тероризм, який характеризується навмисним маніпулюванням і поширенням неправдивої або оманливої інформації, діє як примножувач сили традиційної війни, посилюючи її психологічний, соціальний і політичний вплив.

Розвиток інформаційно-телекомунікаційних технологій суттєво змінив природу сучасних конфліктів. Інформація стала ключовим інструментом сучасної війни.

Сучасна війна все більше покладається на інтеграцію інформаційного тероризму, що включає пропаганду, інформаційно-психологічні операції, кібератаки та дезінформацію, з традиційними військовими операціями. Ці симбіотичні стосунки дозволяють державним і недержавним суб'єктам збільшувати свої досягнення на полі бою, послаблювати моральний дух супротивників і формувати глобальні наративи на свою користь.

У сучасних військових конфліктах кібератаки ефективно використовуються в поєднанні з електронною війною, дезінформаційними кампаніями, протисупутниковими ударами та високоточними боєприпасами. Метою є зниження інформаційної переваги та знищення нематеріальних активів, таких як дані, комунікаційні та розвідувальні системи, а також озброєння, що дає стратегічну перевагу в операціях. Найбільш руйнівні дії, як правило, поєднують високоточні удари з кібератаками для нейтралізації або знищення критично важливих об'єктів. Крім того, кібероперації можуть бути спрямовані на

досягнення політичних цілей, порушуючи фінансові, енергетичні, транспортні та державні інфраструктури з метою ослаблення здатності приймати рішення та спричинення соціальних потрясінь.

Іншою ключовою особливістю цієї взаємодії є використання інформаційного тероризму для прямого доповнення до традиційних бойових операцій. Наприклад, на ранніх етапах російської анексії Криму в 2014 році розгортання так званих «зелених чоловічків» — російських солдатів без розпізнавальних знаків — супроводжувалося потоком дезінформаційних кампаній, покликаних приховати особу та цілі залучених сил [27]. Ця тактика створила тимчасовий інформаційний вакуум, затримавши міжнародну реакцію та дозволивши росії консолідувати свій контроль над регіоном.

Подібним чином у російсько-українській війні кібератаки використовувалися для виведення з ладу української інфраструктури, включаючи енергетичні та комунікаційні мережі. Кібератака у 2015 році на енергетичну мережу України, яку приписують пов'язаним з росією суб'єктам, продемонструвала, як кібертероризм може порушити життя цивільних і послабити стійкість перед кінетичною ескалацією [10]. Ця тактика стерла межі між віртуальною та фізичною сферами, дозволивши інформаційному тероризму посилити психологічний і матеріально-технічний вплив традиційної війни.

Дезінформація є наріжним каменем інформаційного тероризму, який використовується для приховування намірів, заплутування супротивників і маніпулювання міжнародною думкою. Його часто розгортають до та під час військових операцій, щоб дезорієнтувати опонентів і затримати їхню відповідь. Вторгненню росії в Україну у 2022 році передувала масштабна дезінформаційна кампанія, яка зображувала Україну фашистською або нацистською державою та звинувачувала її уряд у геноциді проти російськомовного населення [50]. Ці неправдиві наративи мали на меті виправдати військове втручання перед внутрішньою та міжнародною аудиторією.

Під час активного конфлікту дезінформація продовжує відігравати важливу роль. Спотворюючи реальність, дезінформація дозволяє традиційним військовим діям продовжуватися з обмеженими можливостями.

Громадянська війна в Сирії є прикладом взаємодії між інформаційним тероризмом і звичайними методами війни. Ісламська держава (ІДІЛ) поєднала жорстокі військові кампанії з ефективною пропагандистською машиною, використовуючи платформи соціальних мереж для вербування бойовиків, залякування ворогів і поширення своєї ідеології [70]. Відеозаписи публічних страт і боїв слугували як психологічною зброєю, так і інструментами вербування, посилюючи охоплення та вплив групи за межами поля бою.

Тим часом режим Асада, підтримуваний росією, використовував дезінформацію, щоб приховати використання хімічної зброї, вважаючи винними опозиційні групи [94]. Ці наративи, поширені через державні ЗМІ та соціальні платформи, затримали міжнародну реакцію та дозволили продовжити звичайні військові операції без істотного втручання.

Взаємодія між інформаційним тероризмом і традиційною війною створює зворотний зв'язок, де один посилює інший. Кібератаки та кампанії з дезінформації послаблюють інфраструктуру та моральний дух супротивника, прокладаючи шлях для успішних військових наступів. Пропаганда та ПСО підтримують і посилюють ефекти кінетичних операцій, забезпечуючи довгострокові переваги.

Ця динаміка очевидна в поточному російсько-українському конфлікті, де росія використовує цілісний підхід до війни. Ракетні удари по критичній інфраструктурі супроводжуються кібератаками на системи зв'язку та дезінформаційними кампаніями, спрямованими як на українську, так і на міжнародну аудиторію. Пропаганда, яка зображує українські сили як нелегітимні або неефективні, сприяє підриву впевненості в їхній здатності протистояти, тоді як ПСО намагається використати суспільні розбіжності в Україні та серед її союзників.

Інтеграція інформаційного тероризму з традиційною війною є фундаментальним зрушенням у веденні сучасних конфліктів. Поєднуючи дезінформацію, пропаганду, кібератаки та ІПСО зі звичайними військовими операціями, агресори можуть досягати своїх цілей ефективніше та з меншим опором. Розуміння та протидія цій взаємодії має важливе значення для підтримки глобальної стабільності та захисту демократичних цінностей. Наразі для світової спільноти досить важливо мати чітке усвідомлення про поєднання інформаційних та традиційних засобів ведення війни.

2.3 Прояви державного інформаційного тероризму в конфліктах XXI ст.

Державний інформаційний тероризм означає навмисне використання урядом або державним суб'єктом маніпулювання інформацією, кампаній з дезінформації, кібератак та інших психологічних стратегій, щоб вплинути, порушити або дестабілізувати іншу державу чи населення. Він відрізняється від традиційного тероризму залежністю від некінетичних засобів агресії, які часто відбуваються в цифровому та медіа-ландшафті, а не через фізичне насильство. Ця форма війни може бути спрямована на політичні інститути, соціальну згуртованість, економічні системи та громадську думку з метою досягнення стратегічних переваг без прямого військового протистояння.

Концепція інформаційного тероризму значною мірою спирається на ширшу сферу інформаційної війни, яка охоплює ряд заходів, спрямованих на контроль над потоком інформації, вплив на наративи та виведення з ладу комунікаційних мереж противника. У контексті державних акторів інформаційний тероризм стає потужним інструментом міжнародних відносин, проведення таємних операцій та ведення гібридної війни.

Спонсорований державою інформаційний тероризм став значним інструментом у сучасних конфліктах, особливо в XXI столітті, оскільки країни все більше визнають стратегічну силу впливу на громадську думку, дестабілізації урядів і маніпулювання наративами. У цьому контексті

інформаційна війна, включаючи дезінформацію, пропаганду та психологічні операції, використовувалася державними акторами для досягнення політичних цілей без необхідності прямого військового втручання. Кілька помітних прикладів демонструють зростання керованого державою інформаційного тероризму в сучасних конфліктах.

Одним із яскравих прикладів є використання росією інформаційних операцій під час триваючого конфлікту з Україною, зокрема після анексії Криму в 2014 році та повномасштабного вторгнення в 2022 році. Російський уряд звинувачують у використанні складних методів інформаційної війни для маніпулювання як внутрішньою, так і міжнародною аудиторією. Ці операції включали розповсюдження фейкових новин, використання ботів соціальних мереж і використання тролів, щоб посіяти розкол і плутанину. Мета полягала в тому, щоб підірвати довіру суспільства до українського уряду та міжнародних інституцій, водночас просуваючи проросійські наративи та виправдовуючи військову агресію. Одним з яскравих проявів цього стало використання росією контрольованих державою ЗМІ та онлайн-платформ для поширення неправдивої інформації про ситуацію на сході України, зображуючи її як громадянський конфлікт, а не вторгнення під проводом росії. Ці дії відіграли важливу роль у формуванні наративу навколо анексії Криму та війни на Донбасі, як у росії, так і за кордоном.

Інший приклад у використанні дезінформації під час громадянської війни в Сирії [70]. Уряд Сирії за підтримки свого союзника росії взявся за широке маніпулювання інформацією в рамках своєї стратегії збереження контролю над наративом навколо війни. Сирійський режим використовував державні ЗМІ, щоб демонізувати опозиційні групи, звинуватити їх у тероризмі та представити себе як єдиного законного захисника сирійського народу. Це поєднується з використанням платформ соціальних мереж для поширення провладних повідомлень і посилення контенту, який підриває опозицію. Одним із найефективніших інструментів, які використовував сирійський уряд, було поширення дезінформації, пов'язаної з хімічними атаками в Думі та

Хан-Шейхуні, де уряд звинуватив у цих звірствах опозицію, намагаючись відвернути міжнародну критику [26].

Державний інформаційний тероризм продовжує проявлятися в різних регіонах і конфліктах, часто поєднуючи цифрову тактику з традиційними формами впливу. Ці тактики постійно розвиваються в міру того, як розвиваються технології та коли держави прагнуть отримати перевагу в динаміці глобальної влади.

Державний інформаційний тероризм можна побачити в конфлікті між Сполученими Штатами та Іраном. Після виходу США з ядерної угоди з Іраном у 2018 році [42] Іран все частіше використовує цифрові та медіа-стратегії для протидії політиці США та здійснення впливу в регіоні. Іранські державні суб'єкти застосовували кібератаки для ураження установ США та критичної інфраструктури, одночасно використовуючи платформи соціальних мереж для поширення проіранських наративів. Наприклад, під час загострення напруженості після удару безпілотної США, який убив генерала Касема Сулеймані у 2020 році [12], іранські державні ЗМІ та підтримувані Іраном групи використовували соціальні мережі для посилення антиамериканської позиції та згуртування підтримки уряду всередині країни. Використання цифрових платформ дозволило Ірану обійти традиційні західні медіа-канали та охопити міжнародну аудиторію, поширюючи свою версію подій.

Подібним чином використання Іраном «проксі» інформаційних операцій застосовувалося і в інших частинах Близького Сходу, зокрема в Лівані з Хезболлою та в Іраку з групами ополченців, котрі були прихильниками Ірану. Через цих довірених осіб Іран поширював дезінформацію та пропаганду, щоб дестабілізувати уряди в регіоні, які підтримують західні держави. Як приклад, під час протестів в Іраку в 2019 році [33], коли підтримувані Іраном групи використовували соціальні мережі для поширення дезінформації про протести, зображуючи їх як спроби дестабілізувати Ірак під керівництвом іноземних держав. Контролюючи наратив, Іран прагнув зменшити владу протестувальників і утвердити свій вплив у регіоні.

У випадку Північної Кореї інформаційний тероризм також є важливим інструментом у ширшій геополітичній стратегії держави. Уряд Північної Кореї використовував кібератаки проти Південної Кореї, США та інших супротивників, викрадаючи конфіденційну інформацію, зламуючи фінансові установи та порушуючи цифрову інфраструктуру. Одним із найгучніших інцидентів став злам Sony Pictures у 2014 році, за який Північна Корея взяла відповідальність після того, як компанія випустила сатиричний фільм про північнокорейський режим [46]. Кібератака не лише мала на меті знищити дані та спричинити фінансові збитки, але й послужила формою відплати та засобом контролю за глобальним наративом про лідерство Північної Кореї. Цей напад продемонстрував, що Північна Корея все частіше використовує інформаційну війну як інструмент для помсти за уявні образи та для утвердження влади на міжнародній арені. Це показало, як кібератаки можуть служити засобом залякування, а також засобом придушення свободи вираження поглядів і придушення культурного та політичного інакомислення.

Іншим прикладом є тактика інформаційної війни, яку використовує ізраїльська держава, зокрема в контексті її відносин з Палестиною. Під час військових конфліктів із ХАМАС у Газі Ізраїль постійно використовував засоби масової інформації, щоб сформулювати наратив на користь його дій. Ізраїльські урядові повідомлення, зокрема через соціальні мережі та міжнародні новинні видання, намагалися виправдати військові операції, зображуючи ХАМАС як терористичне угруповання, яке загрожує як ізраїльтянам, так і палестинцям. Складні кампанії Ізраїлю в цифрових медіа відіграли важливу роль у формуванні міжнародного сприйняття, приділяючи особливу увагу висвітленню гуманітарних наслідків дій палестинських бойовиків, применшуючи жертв ізраїльських авіаударів серед цивільного населення. Розглядаючи свої військові операції як захист своїх громадян, Ізраїль використовував інформаційну війну як засіб пом'якшення міжнародної критики та отримання дипломатичної підтримки, особливо з боку західних союзників.

У конфлікті між Туреччиною та курдськими сепаратистами Туреччина залучилася до спонсорованого державою інформаційного тероризму, особливо через соціальні мережі. Турецький уряд використовував традиційні медіа та соціальні медіа, щоб дискредитувати курдські групи, зокрема Робітничу партію Курдистану (РПК), яку Туреччина визнає терористичною організацією [62].

За допомогою кампаній з дезінформації турецька держава намагалася створити наратив, який представляв курдський рух не просто як сепаратистський, а як глобальну загрозу, пов'язану з міжнародним тероризмом. Маніпулюючи інформацією в Інтернеті, Туреччина мала на меті делегітимізувати курдські політичні прагнення та заручитися внутрішньою та міжнародною підтримкою своїх військових операцій проти курдських сил в Сирії та Іраку. Уряд Туреччини також застосував інструменти цифрового стеження та хакерства для моніторингу та придушення активності курдів у соціальних мережах, показуючи, як цифрові платформи можна використовувати для придушення інакомислення та контролю над потоком інформації.

Методи інформаційної війни були використані у конфлікті між Вірменією та Азербайджаном навколо Нагірного Карабаху [17]. Обидві країни використовували кампанії з дезінформації, щоб націлити міжнародну спільноту та сформувані вигідне для кожного з них сприйняття конфлікту. Вірменія, яку підтримує росія, використовувала соціальні медіа і традиційні ЗМІ, щоб представити Азербайджан як агресора, в той час як Азербайджан застосував подібні стратегії, щоб представити Вірменію як загрозу політичній стабільності в регіоні. Під час війни в Нагірному Карабасі обидві країни вели цифрову пропагандистську війну, причому кожна сторона використовувала кіберінструменти для нападу на ЗМІ іншої та поширювала неправдиві повідомлення про військові успіхи та жертви серед цивільного населення. Цифровий і медійний аспекти цього конфлікту показали, як обидві держави намагалися контролювати наратив і маніпулювати сприйняттям війни, щоб виправдати свої військові дії. Також варто зазначити, що не лише одна сторона конфлікту може вдавати до методів інформаційного тероризму, частіше маючи

ресурси та можливості інша сторона теж вдається до інформаційного терору, надаючи конфлікту статусу інформаційної війни.

Представлені вище приклади підкреслюють багатогранність інформаційного тероризму, керованого державою, у XXI столітті. Через маніпуляції в соціальних мережах, традиційний контроль над медіа чи кібероперації державні суб'єкти все більше покладаються на інформацію як на інструмент ведення війни. Метою є не лише контроль над наративом, але й підрив довіри до інституцій, сприяння внутрішньому розколу та послаблення політичних опонентів. Інформація стає дедалі потужнішою зброєю в сучасних конфліктах, тому міжнародне співтовариство стикається зі значними проблемами у протидії цій тактиці й захисті цілісності демократичних процесів.

У 1945 році ООН створювалася як інструмент для управління міждержавними відносинами, коли світ переживав жахи двох світових воєн. Хоча сьогоднішній світ багато в чому безпечніший, природа загроз значно змінилася. Нові, складніші та витонченіші загрози вимагають творчих і сміливих відповідей, а також посилення співпраці між державами, а також приватним сектором і громадянським суспільством.

Спонсорований державою інформаційний тероризм став центральною рисою сучасної війни, коли держави все більше покладаються на кампанії з дезінформації, кібератаки, маніпуляції ЗМІ та психологічні операції для досягнення своїх стратегічних цілей. Конфлікти XXI століття продемонстрували зростаючу важливість інформації як інструменту влади, коли держави використовують ці методи для дестабілізації урядів, впливу на політичні результати та формування глобальних наративів. Оскільки природа конфлікту продовжує розвиватися, роль інформаційного тероризму лише зростатиме, створюючи значні виклики для політиків, військових стратегів і міжнародної спільноти в цілому. Як показує практика, у сучасних конфліктах традиційні методи ведення війни більшою мірою відходять на другий план, в той час як інформаційні атаки керують ходом війни.

РОЗДІЛ 3

ПРОЯВИ ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ У РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ

У російсько-українській війні інформаційний тероризм активно використовується як інструмент агресії з боку росії для досягнення політичних, військових та психологічних цілей. Це явище включає дезінформацію, маніпуляції свідомістю, кіберзагрози та інформаційно-психологічні операції, спрямовані на підрив морального духу українців і дестабілізацію ситуації всередині країни (рисунок Б.2.).

Сучасний російський підхід не новий: він певною мірою повторює марксистсько-ленінські принципи та їхнє відносне бачення істини. Такий підхід не просто відтворює радянське коріння з сукупністю міфотворчості, практик контролю та фундаментальних ідеологічних обмежень, а він адаптує їх до потреб сучасного російського уряду щодо зміцнення державної пропаганди та цензури під час війни, які навряд мали б таку соціальну підтримку в росії без цієї консолідації. Цілком зрозуміло, що навіть російські закони про фейкові новини відіграють значну роль у когнітивній війні росії проти свого населення. Крім руйнівного впливу на свободу слова та демократію в росії, вони допомагають російському уряду збільшити підтримку власного населення щодо путіна та війни в Україні.

Російсько-українська війна підкреслює центральну роль інформації в сучасному конфлікті. Використання росією інформаційного тероризму через дезінформацію, кібератаки та психологічні операції було продуманою спробою дестабілізувати Україну, маніпулювати світовим сприйняттям і досягти політичних цілей. У свою чергу, Україна продемонструвала стійкість проти цієї тактики, використовуючи медіа та цифрові платформи для протидії дезінформації, залучення національної та міжнародної підтримки та збереження свого суверенітету.

Оскільки війна продовжується, стає зрозуміло, що інформаційна війна залишатиметься центральним аспектом конфлікту. Прояви інформаційного тероризму в цій війні служать нагадуванням про зростаючу важливість інформаційного контролю у формуванні результатів сучасних конфліктів і підкреслюють необхідність надійних контрзаходів для захисту цілісності інформації та стійкості суспільств, які піддаються атаці.

3.1. Вплив росії на український інформаційний простір в 1991-2022 роках

З моменту здобуття незалежності України в 1991 році російська федерація систематично здійснювала вплив на український інформаційний простір, прагнучи зберегти культурну, політичну та економічну залежність України. Інформаційна політика росії була спрямована на просування проросійських ідей, дискредитацію проєвропейського курсу України та підрив її суверенітету. Цей вплив еволюціонував від м'якої сили до активного використання дезінформації, пропаганди та кібератак, особливо після Революції Гідності та початку військової агресії у 2014 році.

Після здобуття Україною незалежності у 1991 році російське політичне керівництво намагалося встановити ефективний контроль над політичним розвитком України. Російські політтехнологи — люди, які організовують політичні процеси в суспільстві та організовують комунікацію між владою та народом — брали активну участь у виборчих кампаніях в Україні, наповнюючи їх кремлівськими наративами.

На початку незалежності України росія використала історично сформовану залежність від російського інформаційного та культурного простору. Російські телеканали, такі як «Первый канал» і НТВ, залишалися основними джерелами інформації для значної частини населення, особливо на сході та півдні України. Більшість друкованих видань та радіостанцій також орієнтувалися на російську мову й часто ретранслювали кремлівські наративи. Українська мова лише почала відновлювати свої позиції після років радянської русифікації, а

російська пропаганда акцентувала на «утисках російськомовного населення», намагаючись перешкодити українзації. Крім того, російські фільми, музика, книги та інші культурні продукти значною мірою домінували на ринку, що сприяло збереженню впливу російської ідеології та світогляду серед українців.

У період 2000–2013 років інформаційний вплив росії набув більшого масштабу через розвиток медіатехнологій та політичну напругу, зокрема під час Помаранчевої революції росія активно інвестувала в українські ЗМІ. Проросійські політики та олігархи фінансували телеканали, такі як «Інтер», які транслиували російську версію подій [22]. На українському телебаченні демонструвалися російські серіали та програми, що пропагували ідеї «спільної історії» та «братніх народів».

Під час Помаранчевої революції російські медіа поширювали дезінформацію про масові заворушення та «західне втручання». Проросійські політики в Україні, такі як Віктор Медведчук, активно використовували інформаційний простір для пропаганди ідей федералізації та євразійської інтеграції. росія також застосовувала тактику «підривної інформації», поширюючи фейки про загрози НАТО, націоналістичні рухи в Україні та економічні ризики європейської інтеграції.

Скориставшись політичною нестабільністю в Україні після Євромайдану, наприкінці лютого 2014 року російські війська, перекинуті до Криму під виглядом підрозділів Чорноморського флоту рф, захопили Кримський півострів [12]. Військові діяли у формі без розпізнавальних знаків. Одночасно, серед проросійськи налаштованих мешканців Криму, дезінформованих щодо подій в Україні, були створені збройні формування, які називали себе «самообороною Криму», включно з так званими російськими «козаками».

Також, проводилася операція «Майдан-3», яка була спланована кремлем для провокування ворожнечі та загострення внутрішніх суперечностей в Україні та стала найбільш затратною російською інформаційно-психологічною операцією з 2014 року, за даними ГУР. Редакція видання «Бабель», стверджує, що її загальний бюджет досягнув \$1,5 мільярда [59].

Масштабні дезінформаційні кампанії, організаційна та ресурсна підтримка з боку спецслужб російської федерації, створення незаконних збройних формувань, а також участь регулярних підрозділів російської армії під прикриттям прапорів ополченців Донбасу дозволили захопити частину українських територій та створити маріонеткові квазі-державні утворення. Ці утворення (так звані ЛНР і ДНР) фактично фінансувалися та перебували під зовнішнім контролем російської федерації, що призвело до затяжного військового конфлікту на сході України. За безпосередньої участі РФ не лише імітували події громадянської війни на Донбасі, але й намагалися легітимізувати так звані ЛНР і ДНР як самостійні державні утворення [1].

Події Помаранчевої революції 2004 року в Україні стали важливим фактором для консолідації Росії та її церкви навколо ідеї "російської цивілізації". У той час Українська православна церква Московського патріархату (УПЦ МП) продемонструвала свою підтримку проросійських сил, що підштовхнуло Росію до активного використання РПЦ для поширення ідеології "русского мира". Церква стала важливим елементом у сучасній пропаганді і політиці Росії, включаючи вплив на російську меншину в сусідніх країнах.

Наприкінці 2018 року створення незалежної Православної Церкви України стало серйозною геополітичною загрозою для Росії та РПЦ, оскільки така церква сприяє формуванню національних держав, що є неприємним для Росії (рисунки Б.1.). Після повномасштабного вторгнення Росії в Україну 24 лютого РПЦ ще більше підпорядкувалася режиму Путіна, ставши важливим елементом пропаганди і підтримуючи агресію Росії та злочинні дії, навіть жертвуючи загальнолюдськими цінностями.

У травні 2022 року Патріарх Кирило заявив: «...росія ніколи ні на кого не нападала. Ми ні з ким не хочемо воювати. Це дивно, що велика та могутня країна ніколи ні на кого не нападала – вона лише захищала свої рубежі» [25]. При цьому патріарх Кирило закликав російських вірян до «духовної мобілізації», щоб допомогти військовій мобілізації в Росії. Отже, церква як

пропагандистський інструмент дозволяє росії маніпулювати релігійними почуттями населення для досягнення політичних цілей.

Вже в листопаді 2023 року СБУ повідомила у своєму Telegram-каналі, що оголосили підозру патріарху РПЦ Кирилу, який благословив рашистів на вбивства українців [40]. Було повідомлено про зібрані докази проти глави РПЦ патріарха Кирила (Володимир Гундяєв) за його роль у підтримці військової агресії росії та заперечення військових злочинів, скоєних російськими військами під час вторгнення в Україну.

Використання медіа відіграло важливу роль у сприянні гібридним загрозам через підтримку телеканалів, які контролювалися проросійськими силами. Створення умовного «медіахолдингу Медведчука» на базі телеканалів «112 Україна», «ZIK», «NewsOne», «Перший незалежний» та «UkrLive» [13] створили можливості для донесення ідеологічної позиції кремля не лише до громадян України, а й до представників політичної еліти української держави.

Активне користування соціальними мережами та месенджерами відкрило нове поле для поширення пропаганди, значною мірою замінивши телеканали. Просування в українському інформаційному полі месенджера Telegram, дозволило росії вирішити кілька важливих завдань. Серед них – формування паралельної інформаційної реальності за допомогою анонімних Telegram-каналів і заміна впливових телеканалів Telegram-каналами, які здатні швидше доносити інформацію до споживача інформації. Така комунікаційна активність свідчить про стратегічне значення інформаційного поля в сучасних війнах, а трансформація методів впливу дозволяє говорити про здатність росії підлаштовувати механізми впливу під актуальні завдання.

Одним із показових моментів у цьому питанні можна назвати послідовну дискредитацію полку «Азов» в очах західної спільноти. Російські пропагандисти звинуватили цей підрозділ ЗСУ у «всіх смертних гріхах», але реальність доводить, що ці інсинуації є надуманими [39]. Прикладом є використання провокації з символікою «Азова» під час референдуму в Нідерландах щодо ратифікації Угоди про асоціацію між Україною та ЄС [39].

Російська держава демонструє ефективне використання соціальних медіа в інформаційній війні, використовуючи їх для пропаганди, створюючи дискурс, що викликає розбіжності, і маніпулює як союзниками, так і опонентами за допомогою цілеспрямованих повідомлень [60]. UA War Infographics опублікували графік кількості кібератак РФ у 2021-2023 роках. На ньому помітна тенденція збільшення кількості атак за період трьох років (рисунок Г.4.).

З моменту проголошення незалежності України росія проводила цілеспрямовану інформаційну політику щодо населення Донбасу, спрямовану на зміцнення зв'язків із цим регіоном. Лояльність частини мешканців Донбасу до росії активно використовувалася як інструмент впливу на українську політику, часто ставала важелем маніпуляцій під час виборів різного рівня, а також засобом просування проросійських політичних сил до влади. Після приходу до влади проєвропейських політичних сил унаслідок Революції Гідності 2014 року в частини мешканців регіону виникла стурбованість щодо майбутнього політичного життя країни.

Скориставшись цими настроями, російські спецслужби систематично проводили спеціальні інформаційні операції проти населення Донбасу через засоби масової інформації та інші канали впливу. Ці операції були спрямовані на поширення страхів щодо українських націоналістів, які, за версією російської пропаганди, нібито прийшли до влади в Києві внаслідок державного перевороту (так росія називала Революцію Гідності) і прагнули “розібратися” з російськомовними мешканцями Донбасу. У цьому контексті активно пропагувалася ідея створення так званого «народного ополчення», що додатково стимулювалося економічними проблемами регіону, зокрема зупиненням промислового виробництва, затопленням шахт і загальною неможливістю для цивільного населення знайти офіційне працевлаштування чи отримати легальні доходи.

Російська пропаганда дійсно завжди була спрямована на заперечення української незалежності, представляючи Україну як невід'ємну частину

російської культурної та історичної спадщини. Це проявлялося навіть у привласненні символів української культури, таких як борщ, спотворенні історичних фактів та просуванні наративів про «єдиний народ». Це є елементами інформаційного тероризму, спрямованого на підрив ідентичності України та зміцнення ідеї «русского міра». Це частина ширшої стратегії росії з дестабілізації та ослаблення України.

Привласнення борщу як «російської страви» і просування цього наративу через медіа та офіційні заяви, як от зробило Міністерство закордонних справ рф написавши у твіттері: «Вічна класика, #борщ — одна з найвідоміших і найулюбленіших російських #страв і символ національної кухні» [2], є частиною ширшої стратегії з асиміляції української культури. Ці спроби мають історичні корені, зокрема в радянському періоді, коли культура України систематично підпорядковувалася російській. Одним із пояснень цього явища «привласнення» не лише борщу, але й української історії в цілому, є прагнення росії заперечувати унікальність української культури та підсилювати наратив про «спільне історичне коріння».

В свою чергу, українська сторона ініціювала процес включення культури приготування борщу до Списку нематеріальної культурної спадщини ЮНЕСКО, і в 2022 році це було офіційно визнано, що стало важливим кроком у захисті національної ідентичності [2].

Гібридна війна російської федерації проти України розпочалася ще з моменту проголошення незалежності та утворення суверенної держави, значно активізувалася після Революції Гідності, яка стала результатом масового волевиявлення українського народу щодо геополітичного вибору розвитку країни, та переросла у повномасштабне вторгнення у 2022 році.

3.2 Кібервійна, пропаганда та психологічні операції рф після повномасштабного вторгнення

Особливість російської пропаганди та дезінформації в Україні, особливо під час повномасштабного вторгнення, полягає в її системності, постійності та повторюваності. Існують основні наративи, до яких пропаганда стабільно звертається, а також піднаративи, що використовуються для висвітлення конкретних тем чи повідомлень.

Сьогодні російська федерація активно використовує ідеї радянської пропаганди, а також будує нові міфи навколо подій Другої світової війни, які впливають не лише на український інформаційний простір, а й на міжнародний рівень. Це зумовлено тим, що країна-агресор активно експлуатує стереотипи, що формувалися за часів тоталітарного режиму. Зокрема, часто застосовується так звана анонімна цитата, коли посиляються на неназваних експертів, документи або свідчення без чіткої ідентифікації джерела. Це порушує професійні стандарти журналістики. Окрім цього, у російській пропаганді широко використовуються методи псевдо опитувань і фальшивих рейтингів, метою яких є маніпулювання громадською думкою та спотворення реальності.

Тактика дезінформації російської держави значно розвинулась за останні роки, особливо після вторгнення в Грузію у 2008 році. Вона посилилась під час анексії Криму у 2014 році та активно використовується під час поточних конфліктів в Україні та Сирії. Ці методи є не просто спадком часів холодної війни, а й застосовують великі можливості сучасних технологій та медіа [90].

Від початку повномасштабного вторгнення росія наполегливо поширювала наративи, спрямовані на розпалювання ненависті до України серед своїх громадян. Серед ключових тем – звинувачення в тому, що Україна є центром нацизму та маріонетковою державою, контрольованою Сполученими Штатами. Російські державні ЗМІ, такі як «РБК», підкріпили ці заяви матеріалами, спрямованими на підрив іміджу України та виправдання вторгнення.

Буча, Ірпінь і Гостомель стали символами жахливих злочинів, здійснених російськими військами під час окупації в лютому-березні 2022 року [48]. Після

звільнення цих міст Збройними силами України були виявлені масові вбивства мирного населення, катування, зґвалтування та інші воєнні злочини. Наприклад, у Бучі знаходили тіла мирних мешканців зі зв'язаними руками, а на вулиці Яблунській було виявлено десятки розстріляних людей [35]. Багатьох жертв катували. Виявлено також братські могили, зокрема одну, де було поховано понад 280 осіб [41]. Подібні сцени зафіксовані й у Гостомелі та Ірпені, де масштаб руйнувань і жорстокість окупантів також шокували міжнародну спільноту.

Росія намагалася виправдати свої дії через масовану дезінформацію. кремлівські ЗМІ стверджували, що виявлені трупи — це «постановка» української сторони. Наприклад, у соцмережах поширювали фейкові відео, де нібито «рухаються» тіла загиблих [35]. Ці твердження були спростовані міжнародними медіа та розслідувачами. Також росія заявляла, що українські військові могли бути відповідальними за вбивства, намагаючись дискредитувати докази воєнних злочинів, які підтвердили незалежні організації та ООН.

Ці випадки є прикладом того, як дезінформація може використовуватись для приховування правди про воєнні злочини, маніпулювання міжнародною думкою та виправдання агресії. Водночас об'єктивне документування злочинів допомагає зберігати історичну правду та сприяти справедливості для жертв.

Активне використання ситуації навколо Запорізької атомної електростанції (ЗАЕС) варто трактувати як інструмент інформаційних маніпуляцій і тиску. Після захоплення станції на початку повномасштабного вторгнення [8], російські військові перетворили її на військовий об'єкт, що створило значні загрози для безпеки регіону. Москва поширювала дезінформацію про можливі атаки Збройних сил України на АЕС [8], зокрема звинувачуючи Київ у планах зруйнувати станцію, хоча докази вказують на те, що це були російські провокації.

Особливу небезпеку становило мінування критичних частин станції, включно з басейнами-охолоджувачами і реакторами [8]. Міжнародні експерти наголошували, що руйнування цих об'єктів може викликати катастрофічні

наслідки, зокрема значне радіоактивне забруднення великих територій, що нагадує сценарії аварій на Фукусімі чи Чорнобилі. Ці загрози росія використовувала для тиску на міжнародну спільноту з метою стримання українського контрнаступу в регіоні.

Маніпуляції кремля включали залякування європейських країн потенційною радіаційною катастрофою, що могло би зачепити і їхні території. Такі дії є прикладом ядерного шантажу, спрямованого на зміну ходу війни. При цьому українська сторона постійно інформувала міжнародних партнерів і організації про реальну ситуацію та викривала російські фейки, зокрема на дипломатичному рівні через МАГАТЕ та інші міжнародні структури.

На думку авторки магістерського дослідження, роль ЗАЕС у цій війні стала одночасно військовою, економічною та інформаційною: російські війська використовують її як базу, блокують доступ до української енергетики, а також поширюють дезінформацію з метою посилення глобальної напруги.

У подальшому інформація про ці та інші трагедії використовуватиметься в медіа та соціальних мережах як одне з джерел або інструментів інформаційного тероризму. Наприклад, російські ЗМІ часто публікують наративи, в яких звинувачують Україну у фінансових та етичних порушеннях. В одному випадку «РБК» стверджував, що Україна безоплатно крала газ у російського «Газпрому», виставляючи українську державу ненадійною та корумпованою. Ще одним прикладом систематичних інформаційних кампаній Російської Федерації стала фейкова новина одного з російських ЗМІ про нібито розп'ятого військовослужбовцями ЗСУ хлопчика [19].

Такі маніпулятивні наративи російські медіа поширюють роками, формуючи у громадян росії ненависть до українського народу. За допомогою вигаданих історій та фейкових сюжетів кремлівська пропаганда прагне виправдати та приховати воєнні злочини, скоєні російськими військовими на території України. Основна мета таких дій - створити у громадян росії хибне уявлення про перебіг війни та зобразити українців у негативному світлі. Для

цього пропагандистські ресурси використовують неправдиві усні та письмові повідомлення, а також постановочні відеоматеріали.

Серед найбільш поширених фейкових повідомлень можна виділити пости у соціальних мережах, таких як Facebook і Telegram, а також матеріали на YouTube та Instagram. Ці платформи є особливо ефективними для поширення маніпулятивної інформації, оскільки аудіовізуальний контент легше сприймається і привертає увагу великої аудиторії.

Через значний час, який люди проводять в Інтернеті, і відсутність жорсткої цензури або авторитетного лідерства думок, саме соціальні мережі сприяють швидкому поширенню дезінформації, на відміну від традиційних медіа. Месенджери, такі як Viber, WhatsApp і Telegram, часто розглядаються користувачами як приватний простір. Це робить їх особливо ефективними для передачі фейкових повідомлень, створення паніки, розпалювання ворожнечі або залякування.

Окрему загрозу становлять фальшиві SMS-повідомлення, які часто орієнтовані на літніх людей, що рідше користуються іншими формами Інтернет-комунікацій. Такі повідомлення використовуються для маніпуляцій, поширення чуток або паніки серед вразливих верств населення.

Не важко помітити, як сильно активізувалася діяльність російської та української пропаганди в соціальних мережах, особливо в X (колишній Twitter), адже вони дають можливість впливати не лише на населення обох держав, а і на міжнародну спільноту в цілому. Проукраїнські твіти підкреслюють єдність у підтримці проти російської агресії, вважаючи проросійську позицію злочинною. Водночас проросійські твіти зображують український уряд як “нацистський” і корумпований, звинувачуючи його у зраді історичної єдності з росією. Цей наратив намагається виправдати російське втручання як захист від цієї зради.

Проукраїнський наратив акцентує увагу на стражданнях цивільного населення та турботі про людське життя, зображуючи росію як агресора, порівнюючи її з історичними тиранами, такими як Гітлер. Це подання спрямоване на виклик співчуття та підтримки України, представляючи конфлікт

як несправедливу агресію. Натомість проросійський наратив виправдовує дії режиму путіна як захист російськомовного населення України, вважаючи військові дії необхідними для запобігання більшій шкоді. Це протистояння у трактуванні турботи та шкоди відображає конфлікт навколо морального обґрунтування війни.

Фейки поширюються не лише в соціальних мережах, але й через традиційні ЗМІ. Російська пропаганда активно використовує маніпулятивні новини на різні теми, зокрема спрямовані на дискредитацію Збройних сил України та переселенців із зон активних бойових дій. Кремлівські ЗМІ намагаються сформувати негативний образ українських військових в очах громадськості. Типовими ознаками таких фейків є використання маніпулятивних фраз, таких як “достовірна інформація”, “мені сказали військові” або “ви мене знаєте, я не буду брехати”. Джерелами таких новин часто називають “ексклюзивні дані від знайомих”, “родичів у прокуратурі” або “джерела у вищих колах”.

Російські ЗМІ, маніпулюючи фактами, поширювали інформацію про те, що Велика Британія і Туреччина нібито планують скупити все українське зерно, прирікаючи Україну на голод. Вони посилялися на заяву міністра закордонних справ Великої Британії Ліз Трасс [3]. Проте насправді в її заяві йшлося про співпрацю між цими країнами та Україною для забезпечення експорту зерна.

Подібним чином російські пропагандисти маніпулювали ситуацією зі шоломом NGU-56/P АВН, знайденим на місці падіння українського гелікоптера. Ці шоломи використовують пілоти країн-членів НАТО та армії США, але не українські військові. Пропаганда поширювала звинувачення про участь НАТО у війні в Україні, використовуючи це як доказ [44]. Пізніше було з'ясовано, що фото шолома вперше опублікувала компанія Gentex Corporation — виробник цього спорядження. Знімок був зроблений і переданий ВПС України як подяка за те, що шолом врятував життя пілота [44].

Держава-агресорка використовує інформаційні атаки в поєднанні з ракетними обстрілами. Це особливо помітно на прикладі атак на зернову

інфраструктуру, які відбулися після її виходу росії із Зернової угоди. Агенція Top Lead зазначає: відразу після виходу росії із Зернової угоди, наступним її кроком була ракетна атака на зернову інфраструктуру в Одесі, після чого вона почала активно поширювати фейки про те, що інфраструктура була військова, а ніяк не аграрна (рисунки Г.5.). І в такому темпі вона продовжувала роздувати дезінформацію щодо цього питання.

Сьогодні, особливо у воєнний час, поширеним способом маніпуляції став фішинг — вид шахрайства, спрямований на викрадення персональних даних. Основна мета фішингових повідомлень — обманом змусити людину швидко перейти за підробленим посиланням і ввести конфіденційну інформацію, таку як дані банківської картки (номер, термін дії, CVV-код тощо).

Сайти, на які ведуть такі посилання, зазвичай імітують офіційні ресурси, зокрема Кабінет Міністрів, українські міністерства, банки або міжнародні організації, як-от ООН, ЮНІСЕФ чи ЄС. Типовими ознаками фішингу є вигадана історія про виплати фінансової допомоги для постраждалих від війни, наявність посилання для введення персональних даних, коментарі ботів про те, що виплати вже отримали інші, та обмеження часу на виконання дій, щоб не дати людині можливості обдумати ситуацію.

На жаль, понад 5 тисяч українців стали жертвами таких схем. Під виглядом соціальних виплат шахраї ошукали громадян на понад 100 мільйонів гривень [11]. Щоб уникнути подібних ситуацій, важливо завжди перевіряти достовірність інформації та уникати переходів за сумнівними посиланнями.

У травні 2022 року в Україні ухвалили закон №2243-IX [29], який розширює підстави для заборони політичних партій, які виправдовують російську агресію, заперечують окупацію українських територій або зображують війну як внутрішній конфлікт. У результаті 12 проросійських партій, зокрема «Опозиційна платформа – За життя» та «Партія Шарія», були заборонені за антиукраїнську пропаганду [29]. Після ухвалення закону міжнародні ЗМІ висловили занепокоєння щодо цензури, відволікаючи увагу від зусиль України щодо боротьби з російськими шпигунськими мережами.

Один із методів, які використовує росія, — поширення відеозаписів і фото з тортурами або стратами українських військових. Наприклад, у 2023 році у соціальних мережах поширювалося відео з обезголовленням українського військовополоненого. Ці матеріали поширювалися через проросійські Telegram-канали, маючи на меті залякати українців і деморалізувати армію [4]. Крім того, такі дії спрямовані на створення відчуття безпорадності серед цивільного населення, викликаючи страх за долю близьких, які перебувають на фронті.

Російська пропаганда активно просуває тезу про соціальну несправедливість між тими, хто воює, і тими, хто уникає мобілізації. Такі наративи підсилюються історіями про українців, які виїжджають за кордон, залишаючи співвітчизників на самоті у боротьбі за незалежність. У соціальних мережах і ЗМІ поширюються матеріали, які викликають роздратування і злість серед мобілізованих та їхніх родин, порівнюючи їхню важку долю з «безтурботним життям» ухильників [9]. Це підживлює внутрішній конфлікт і знижує довіру до державних інститутів, відповідальних за мобілізацію.

Росія постійно акцентує увагу на мовному питанні, намагаючись створити в Україні розкол між російськомовними і україномовними громадянами. Наприклад, в окупованих регіонах активно поширюються наративи про «примусову українізацію», яка нібито загрожує російськомовним громадам. Ці фейки спрямовані на підриг єдності українського суспільства та формування недовіри до центральної влади.

Регіональний розкол також активно підтримується через міф про «особливість» півдня і сходу України. У російських ЗМІ просувається теза, що ці регіони нібито історично ближчі до росії і мають право на самовизначення. Це використовувалося як виправдання для окупації Донбасу та Криму, а також для легітимізації псевдореферендумів на інших територіях.

Російська інформаційно-психологічна операція під назвою «Фортеця Львів» мала на меті посіяти розбрат серед українців, акцентуючи на нерівномірності страждань у регіонах України через війну [45]. Пропаганда

спрямовувалася на створення напруги між мешканцями західних і східних областей. Зокрема, у TikTok активно поширювали відео, які саркастично висвітлювали ситуацію у Львові, висміюючи його «привілейоване» становище [45]. Російські боти використовували жарти про «захмарні ціни на оренду» і намагалися протиставити це стражданням жителів Маріуполя чи Бахмута, що пережили значні руйнування та гуманітарні кризи.

Особливою формою маніпуляції стали відео, які висміювали популярну пісню «Фортеця Бахмут» гурту «Антитіла», замінюючи її на «Фортеця Львів». Під такими відео залишали коментарі, які принижували значення західного тилу, позиціонуючи Львів як «безтурботний» і «далекий» від війни. Ці дії спрямовувалися на те, щоб викликати у мешканців інших регіонів почуття несправедливості та створити емоційну напругу між регіонами України.

Такі провокації також використовувалися для дискредитації єдності України і стимулювання недовіри до західних союзників, зокрема Польщі, через наративи про нібито можливі територіальні претензії до Львівщини. Це мало на меті підірвати співпрацю між Україною та її міжнародними партнерами, водночас поглиблюючи регіональні конфлікти всередині країни.

За даними «Детектор медіа» в рамках проєкту «Disinfo Chronicle» з початку повномасштабного вторгнення та станом на 10 листопада 2024 року редакція зафіксувала: 2512 фейків, 749 маніпуляцій, 734 меседжів та 535 викриттів (рисунок Г.2.). Ці випадки демонструють, як інформаційна війна може бути використана для дестабілізації суспільства під час збройного конфлікту, сприяючи розколу і недовірі серед населення.

На різних етапах російсько-української війни, кремлівські наративи, керовані ботами, стратегічно намагалися вплинути на сприйняття та думки громадськості. Під час фази вторгнення проросійські боти дискредитували НАТО та згуртовували підтримку росії, тоді як проукраїнські боти наголошували на необхідності протистояти російській агресії та зосереджувалися на гуманітарних питаннях. У міру ескалації конфлікту проросійські наративи посилювали паплюження України за допомогою історичних

антагонізмів. Натомість проукраїнські боти засудили російське керівництво та наголосили на відповідальності. Під час Херсонського контрнаступу проросійські боти посилювали розкольніцьку риторику, щоб підірвати українську єдність, тоді як проукраїнські боти наголошували на кримінальній відповідальності та доблесті.

Після ескалації російських дезінформаційних кампаній, що посилювалися після повномасштабного вторгнення в Україну у лютому 2022 року, українська сторона почала відповідати більш жорсткими заходами. Україна посилала свою інформаційну та медійну стійкість, впровадивши контрзаходи проти російських наративів, зокрема шляхом поширення достовірної інформації та контролю діяльності медіа, пов'язаних з росією.

3.3. Боротьба України з російським інформаційним тероризмом в умовах війни

Боротьбу України з російським інформаційним тероризмом варто вважати центральним компонентом оборонної стратегії в умовах війни. Проаналізувавши діяльність росії в цьому напрямку, стає зрозумілим що, російська інформаційна війна набула ознак інформаційного тероризму й була однією з ключових тактик москви задовго до повномасштабного вторгнення 2022 року. Ці кампанії спрямовані на спотворення правди, насичення інформаційного простору фейками, створення плутанини, маніпулювання як українською, так і міжнародною аудиторією. Розуміння та протидія цій загрозі є важливими для стійкості України та її здатності протистояти російській агресії.

Росія як держава-терорист активно використовує інформаційну сферу. Мета російського інформаційного тероризму полягає в тому, щоб дискредитувати Україну та вплинути на її закордонних партнерів. Звичайні методи російської пропаганди, такі як просування відвертої брехні, втрачають свою ефективність серед більшості українців, які виробили певний «імунітет» до дезінформації кремля під час повномасштабного вторгнення. Наразі помітно,

що російські пропагандисти намагаються використати у власних цілях реальні проблеми, з якими стикаються українці, хоча й інтерпретують це через власну призму. Вони зосереджуються на наративах навколо масової мобілізації, широко поширеної корупції в Україні, уявного «провалу» контрнаступу Збройних Сил України та нібито відсутності довіри до України серед західних партнерів [47].

За словами засновниці ініціативи «НотаСнота» Альони Романюк, протягом 2022 року росія витратила на просування пропаганди через державні медіа \$1,9 млрд замість запланованих \$1,5 млрд. [37]. У цю суму не входять соціальні мережі, пропаганда через кіно, ботоферми, витрати на пропаганду через освіту, а лише державні медіа.

На законодавчому рівні в Україні відсутнє чітке визначення інформаційного тероризму. За словами Б. Леонова та С. Лихової, закон України «Про боротьбу з тероризмом» містить поняття «технологічний тероризм», яке не збігається з дефініцією «інформаційний тероризм», а Закон України «Про основні засади забезпечення кібербезпеки України» містить визначення «кібертероризму», який можна визнати лише одним із різновидів інформаційного тероризму [21]. Варто зауважити, що міжнародні правові акти також не містять визначення інформаційного тероризму, серед них, зокрема, Конвенція Ради Європи про запобігання тероризму (2005 р.) та Конвенція про кіберзлочинність (2001 р.).

Чіткої, розробленої стратегії для боротьби з російським інформаційним тероризмом наразі немає. Незважаючи на це, державні та незалежні структури докладають максимум зусиль, щоб відбивати російські інформаційні та кібератаки. Потужна мережа організацій, таких як Detector Media, StopFake і VoxCheck, активно аналізує дії противника та створює текстовий, аудіо- та відеоконтент різними мовами.

Стратегічні ініціативи з протидії дезінформації впроваджені на рівні уряду. Центр протидії дезінформації при Раді національної безпеки і оборони України та Центр стратегічних комунікацій та інформаційної безпеки

Міністерства культури та інформаційної політики є головними державними структурами, що здійснюють боротьбу з інформаційним тероризмом росії на регулярній основі. Вони змінюють ключову роль у боротьбі з дезінформацією і створюють вагомий внесок у зміцнення інформаційної стійкості українського суспільства.

Сучасна популяризація соціальних медіа в суспільстві дає можливості як і для державних, так і для незалежних медіа поширювати правдиву інформацію та руйнувати російські ІПСО. За даними Київського Міжнародного інституту соціології, який проводив опитування на замовлення Програми розвитку ООН в Україні за підтримки Швеції й у партнерстві з Міністерством цифрової трансформації України, станом на 2023 рік відсоток українців, які кожного дня користувалися інтернетом, зріс до 80% (у 2022 році цей показник становив 72%) [43]. Це означає, що все більша кількість громадян України потенційно може стати жертвами інформаційних атак агресора.

Боротьба з російською дезінформацією в соціальних медіа стала все більш актуальною з початком повномасштабного вторгнення. Не лише державні структури, а і українські активісти та впливові особи намагаються руйнувати російські наративи, що нав'язуються українському суспільству щодня. Державні діячі та структури активно ведуть сторінки в Instagram і X (колишній Twitter), де стають більш відкритими та ближчими із суспільством і мають змогу, поширюючи інформацію, впливати на міжнародну спільноту, залучати власних громадян. Facebook дозволяє поширювати вплив на людей старшого віку. Провідні державні діячі ведуть Telegram або Youtube-канали, де більш детально описують, коментують та проводять аналіз новин для суспільства, цим самим руйнуючи російську пропаганду.

До прикладу, відомий український інфлюенсер, Ігор Лаченков, разом зі своєю командою, створив спеціальний канал «Lachen Bots» (рисунок А.1) для швидких та скоординованих дій в інформаційній боротьбі. Метою даної спільноти є протидія російській пропаганді. В телеграм-каналі чітко прописуються дії, які може робити кожен громадянин, котрий хоче допомогти в

руйнуванні російської пропаганди в соціальних мережах, шляхом інформаційних атак та скарг на сторінки російських діячів та медійних осіб. Підписники поширюють інформацію про російсько-українську війну для міжнародної аудиторії, щоб західний світ більше знав про терористичну діяльність росії. Так як рф, почала активно створювати фейкові акаунти, та поширювати неправдиву інформацію щодо війни в Україні, така діяльність з боку українських громадян є важливою та не менш впливовою на хід інформаційної війни росії з Україною.

Необхідно наголосити, що після повномасштабного вторгнення українське суспільство активізувалося в боротьбі з усім російським. Вся пропаганда яка існувала серед людей, та нав'язувалася росією століттями активно руйнується. Після того як російські наративи почали витісняти з інформаційного простору України, велика кількість українських діячів спрямували свою діяльність для розвитку та поширення всього українського.

Першим важливим інструментом у протидії російській дезінформації став кінематограф. Фільми, створені українськими та міжнародними режисерами, не лише висвітлюють реальність війни, а й руйнують пропагандистські наративи кремля, доносячи правду до міжнародної аудиторії. Одними з таких фільмів варто виділити документальний фільм Мстислава Чернова «20 днів у Маріуполі» (рисунок В.2.), який руйнує наративи кремля про «визвольну місію» та доводить, що російська агресія спрямована на знищення українських міст і цивільного населення, фільми «Щедрик» (рисунок В.3.) та «Конотопська відьма» (рисунок В.4), що використовуються як культурний інструмент для протидії російській пропаганді. Стрічки підкреслюють унікальність української культури та національної ідентичності. Також, кінострічка «Заборонений» (рисунок В.1), що є культурною відповіддю на російську пропаганду та відроджує пам'ять про українських поетів та дисидентів і розкриває правду про радянські злочини, зміцнюючи національну свідомість і сприяючи формуванню історичної правди.

Важливу роль відіграють об'єднання творчих людей, головна ціль яких повернути популяризацію української мови, культури та історії. Одним з таких об'єднань став український гурт "МУР" назва якого відсилає до харківського Мистецького Українського Руху 1940-х років, а також символічно натякає на «мур» — захисний бар'єр проти російської агресії та культурної асиміляції. Ним був випущений перший в Україні історичний альбом-мюзикл «Ти [Романтика]» (рисунок В.5.) про розстріляне відродження, який розвінчує міф про «єдину культуру» та «спільну історію» з росією та демонструє силу українського мистецтва навіть в умовах війни.

На законодавчому рівні також відбуваються зміни, що сприяють боротьбі з російськими наративами. У січні 2023 року було подано законопроект №8371 [7], який забороняє діяльність релігійних організацій, підконтрольних державі-агресору. Цей закон спрямований, зокрема, проти Української православної церкви Московського патріархату (УПЦ МП), що підпорядковується Російській православній церкві (РПЦ). Схвалення даного законопроекту відбуло 20 серпня 2024 року [31], напередодні Дня Незалежності України і стало ще одним кроком до руйнування російського впливу на Україну.

Також, не менш важливим стало набуття чинності статей котрі входять до Закону України “Про забезпечення функціонування української мови як державної”, а саме Стаття 25 [30], яка регламентує використання державної мови у сфері друкованих медіа, зокрема містить вимоги щодо їх виготовлення, опублікування та розповсюдження. росія довгий час використовувала мовний і культурний поділ як клин, щоб посіяти розбрат в українському суспільстві, особливо між російськомовним сходом і україномовним заходом. Закон ускладнив домінування російськомовних ЗМІ та підтримуваних росією культурних елементів, а також розриває умовні «кабелі» через які росія постійно вливала велику кількість дезінформації та пропаганди.

Зі свого боку Україна теж вдається до кібератак і на державному рівні, які мають певний успіх. До прикладу, А. Крижний у своїй статті розповідає про масштабну кібератаку, яка була організована Головним управлінням розвідки

Міноборони України, що паралізувала роботу ключових банківських установ і платіжних систем по всій території росії. Як зазначає автор статті, російська влада визнала факт кібератаки, назвавши її справою рук «політично мотивованих хакерів», а в українській розвідці зазначали, що атака далека до свого завершення [20].

Центр протидії дезінформації був створений в Україні у березні 2021 року згідно з Указом Президента України №106/2021 [32]. Його основна мета – забезпечення інформаційної безпеки України, протидія дезінформації, пропаганді та деструктивним інформаційним кампаніям. Центр є складовою апарату Ради національної безпеки і оборони України (РНБО) і працює над координацією органів виконавчої влади у сфері інформаційної безпеки.

Одним із головних чинників які впливають на підривання російської пропаганди є успішні операції ЗСУ на фронті. Після перетину російсько-українського кордону Збройними силами України, розпочалася «курська операція», яка зруйнувала наратив про «перемогу» росії, а також підірвала імідж путіна як лідера ядерної держави. Операція створила негативні зміни в психологічному стані населення рф та дозволила українській пропаганді краще впливати на російське суспільство та підривати довіру до кремля зсередини держави.

Підсумовуючи, зазначимо, що боротьба з російським інформаційним тероризмом – це довгострокова стратегія, оскільки дезінформації набагато важче протистояти, ніж фізичним загрозам. Росія розробила складні методи впливу на думки та позиції людей за допомогою інформації та для посилення інформаційного хаосу. Незважаючи на успішні контрзаходи України, збереження громадської довіри та міжнародної солідарності залишається проблемою, особливо в умовах, коли війна далека від свого завершення, а втома від неї поширюється як всередині держави, так і за її межами.

3.4. Вплив російського ІПСО на думку міжнародної спільноти щодо російсько-української війни

Російські ІПСО є важливим інструментом у веденні гібридної війни проти України та спрямовані на формування хибного сприйняття війни серед міжнародної спільноти. За допомогою дезінформації, маніпуляцій та пропаганди кремль намагається створити вигідні для себе наративи, які впливають на світову громадську думку, міжнародні організації та уряди інших держав.

Одним із головних механізмів впливу є поширення дезінформації через міжнародні медіа, такі як RT та Sputnik. Ці канали активно транслюють спотворену інформацію, наприклад, про “нацизм” в Україні або “геноцид” російськомовного населення на Донбасі. Класичним прикладом є вигадана історія про “розп’ятого хлопчика” в Слов’янську у 2014 році, що мала на меті викликати емоційний відгук у міжнародній аудиторії. Також росія використовує соціальні медіа, ботів і тролів для поширення фейкових новин та створення інформаційного шуму. Наприклад, кампанія #IStandWithRussia була організована з використанням ботів для демонстрації нібито міжнародної підтримки рф [86].

Ще одним інструментом є створення фейкових акаунтів експертів і очевидців, які поширюють вигідні для росії меседжі. Ці акаунти часто зображають конфлікт як внутрішню українську кризу, що виправдовує втручання росії. Окрім того, рф активно дискредитує західні держави та НАТО, стверджуючи, що підтримка України є вигідною лише Заходу, і створюючи міфи про “чорний ринок зброї” в Україні.

Росія активно використовує кінематограф і музику як інструменти “м'якої сили”, спрямовані на поширення своїх пропагандистських наративів і формування позитивного іміджу на міжнародній арені. Ці сфери культури стають важливими засобами впливу на світову аудиторію, а також на утвердження ідеологічних установок як всередині країни, так і за її межами.

Нещодавна новина про показ фільму «Глухі коханці» режисера-росіянина Бориса Гуца з російськими акторами про любов між україркою і росіянином в Стамбулі на Талліннському кінофестивалі викликала бурю негативних емоцій в українців. Через цей фільм, Гуц заявив, що хотів створити фільм, який показує, як війна руйнує людяність і, що найважливіше, вона вбиває любов [80]. На думку авторки кваліфікаційної (магістерської) роботи, створення цієї кінострічки варто вважати проплаченим та замовленим росією. Представивши світу фільм, де українка кохає росіянина, росія вкотре планує показати світу про «бажання України та росії бути одним цілим та існувати в мирі і злагоді». Навіювання людям такого наративу, дасть уявлення про бажання росії швидше закінчити війну та відновити з Україною «стару дружбу».

Результатом таких дій є вплив на сприйняття війни міжнародною спільнотою. Зокрема, дезінформація допомагає створити уявлення, що конфлікт є суто внутрішнім питанням України, що підриває західну підтримку. Також пропаганда рф сприяє зростанню скептицизму щодо санкцій проти росії, формуючи думку, що вони більше шкодять країнам Європи, ніж росії. Ще одним наслідком стало поляризація суспільства в демократичних країнах, коли окремі політичні рухи або партії починають транслювати проросійські меседжі.

У Європі росія регулярно поширювала інформацію про те, що Україна продає західну зброю для отримання прибутку на міжнародному чорному ринку, намагаючись підірвати європейську підтримку Україні. Крім того, росія активно просувала наратив про те, що країни Європейського Союзу зазнають серйозних труднощів взимку без постачання російського газу, запустивши велику онлайн-кампанію з використанням понад п'ятдесяти фейкових вебсайтів, які видають себе за авторитетні європейські ЗМІ.

Операції росії не обмежувались лише європейськими країнами, що допомагали Україні зброєю та фінансами. росія активно поширювала свої наративи на Південному Кавказі та в Молдові, маючи на меті не лише ослаблення підтримки України, а й розкол суспільств всередині цих країн для здобуття місцевого впливу. Наприклад, вірменські проросійські активісти

використовували критику прем'єр-міністра Нікола Пашиняна після того, як Азербайджан завоював Нагірний Карабах, аби підбурювати до антиурядових настроїв [54]. В Азербайджані росія використовувала російськомовну аудиторію та наукові кола, щоб посилити свій вплив через відсутність незалежних ЗМІ. У Сакартвело уряд після повномасштабного вторгнення росії в Україну розширив співпрацю з Москвою, використовуючи страхи населення щодо ескалації війни для зміцнення проросійської позиції. У Молдові росія застосовувала енергетичний шантаж і поширювала неправдиві наративи про військову загрозу від України чи НАТО для сепаратистського регіону Придністров'я [99].

Бен Дженсен з CSIS в своїй доповіді зазначив те, що попри невдачі росії на полі бою в Україні та зростаюче невдоволення всередині країни, ставлення до росії в країнах Глобального Півдня стає дедалі позитивнішим [63]. Використання ферми тролів, доступ до RT в Африці та ефективна комп'ютерна пропаганда сприяють формуванню форми Москви як жертви західного неоімперіалізму. У таких наративах Путін виглядає більш як сучасний Че Гевара, а не старіючий авторитарний лідер. Потужний потік глобальної пропаганди ускладнює роботу програми розвитку США і може призвести до протестів біля американських посольств за кордоном. КНР також активізує ці зусилля, посилюючи невдоволення в Південно-Східній та Центральній Азії, а також в Латинській Америці [63].

Дослідження *The Economist* показало, що російська пропаганда активно впливає на соціальні мережі в Азії та Африці [92]. Автори аналізували 7,7 тисяч акаунтів і виявили, що в Індії поширюються наративи, які стверджують, що НАТО мало б вести переговори з росією на основі її пропозицій [92]. Пропаганда поширює інформацію про те, що українці використовують індійців як «живий щит», що шкодить братерським відносинам між росією та Індією. В Африці російські пропагандисти акцентують увагу на «злочинах» НАТО в Лівії, Іраку, Афганістані та Сирії, стверджуючи, що Альянс вбив 1,6 мільйона осіб [92]. Вони порівнюють міжнародну реакцію на ці події з тим, як світ реагує на загибель 200 українських солдатів. У цих регіонах росія активно просуває образ

НАТО як імперіалістичної та колоніальної сили, намагаючись посіяти ворожнечу між західними країнами та місцевими суспільствами. Цікаво, що 52% акаунтів, що брали участь в поширенні цих повідомлень, належать звичайним користувачам, що свідчить про масштабність цієї пропагандистської кампанії (рисунок Г.3.).

Російська пропаганда має на меті заповнити увесь світ та підірвати образ України на міжнародній арені, а також створити таке міжнародне середовище в якому Україна не буде отримувати допомоги та підтримки від Західного світу. Хоча росія вливає в пропаганду та поширення дезінформації мільярди доларів, демократичні держави не піддаються цій інформаційній «брехні».

Центр Протидії Дезінформації повідомив про те, що глава Міністерства закордонних справ російської федерації сергій лавров дав інтерв'ю одному з американських видань, використавши цю нагоду для поширення кремлівської пропаганди серед західної аудиторії . лавров висунув російський ультиматум, представивши його як «умови для врегулювання конфлікту», що включають вимогу від України передати свої території москві та прийняти інші незаконні вимоги агресора.

Оприлюднені заяви лаврова ще раз підтверджують, що росія не має наміру мирно врегулювати конфлікт, а вимагає капітуляції України та визнання незаконного захоплення її територій. лавров намагався зобразити Україну як «агресора» виключно через збройне вторгнення України в Курську область, хоча саме росія окупувала українські території та продовжує вести бойові дії. Погрози, висловлені лавровим на адресу Заходу, здебільшого стосуються можливості дозволу Україні завдавати удари по території росії із західною зброєю.

Агресивна політика росії, байдуже ставлення до закликів Заходу щодо припинення війни на території України та залучення Північної Кореї у війну з Україною призвело до того, що 17 листопада 2024 року The New York Times опублікували статтю в якій зазначалося, що за повідомленнями офіційних осіб США, президент Байден вперше надав дозвіл Україні використовувати надані

Сполученими Штатами ракети великої дальності для ударів вглиб території росії [66].

Стаття, опублікована на платформі «Детектор медіа», детально аналізує сучасні проросійські інформаційні стратегії у Центрально-Східній Європі (ЦСЄ), зокрема їхні методи, тематику та ключові меседжі [5]. Дослідження зосереджується на інформаційному просторі регіону у січні 2024 року, розкриваючи масштабність і вплив цих стратегій на суспільну думку.

Детектор медіа за даними LetsData проілюстрував динаміку публікацій про Україну у січні 2024 у країнах ЦСЄ в соціальних мережах (рисунк Г.6.). На графіку публікацій, сформованому на основі даних, видно кілька незначних піків у кількості ймовірних дезінформаційних повідомлень та один значний сплеск 24 січня, який збігся з падінням російського літака Іл-76 у Белгородській області [5].

Російська пропаганда адаптує свої меседжі залежно від конкретної країни. До прикладу в Польщі наголошується на загрозах з боку українських мігрантів та історичних конфліктах. Словаччина та Угорщина наповнюється контентом щодо невдоволення політикою ЄС і «традиційні цінності», а в Балканських країнах використовує тему «слов'янського братерства» та релігійної єдності [5].

Також звертається увага що ЄС та НАТО вже впроваджують низку ініціатив для протидії російській пропаганді створюючи фактчекінгових платформ, таких як EuvsDisinfo, посилюють кібербезпеку та розробка інформаційної політики, а також співпрацюють з місцевими урядами для підвищення медіаграмотності населення [5]. Водночас темпи впровадження цих заходів не завжди відповідають швидкості поширення дезінформації.

Загалом, російські ІПСО має значний вплив на формування міжнародної думки щодо війни в Україні, проте ефективна протидія дезінформації з боку України та її союзників зменшує цей вплив. Боротьба з пропагандою є важливим елементом сучасної гібридної війни, і міжнародна спільнота дедалі більше усвідомлює необхідність спільних зусиль для руйнування російських наративів.

Таким чином, прояви інформаційного тероризму в російсько-українській війні мають значний вплив на хід конфлікту. Одним із основних методів є поширення фейкових новин та маніпуляцій, які мають на меті змінити сприйняття реальності як в Україні, так і в міжнародному просторі.

Особливу роль відіграють кіберзагрози та атаки на критичну інфраструктуру, які паралізують систему управління, порушити зв'язок між різними державними інститутами та навіть викликати паніку серед населення. Росія активно використовує хакерські атаки для збору розвідданих, а також для того, щоб завдати шкоди українським державним і приватним установам. Ще одним важливим елементом є психологічні операції, що спрямовані на маніпуляцію громадською думкою та підлив національної єдності в Україні.

Україна, своєю чергою, активно реагує на ці загрози. За допомогою власних медіа-ресурсів, цифрових платформ і спеціальних програм боротьби з дезінформацією, країна намагається нейтралізувати вплив ворожих інформаційних атак.

Важливою частиною боротьби з інформаційним тероризмом є міжнародна підтримка. Війна в Україні показала, наскільки важливими є міжнародні інформаційні та технологічні мережі для відбиття зовнішніх інформаційних атак. Таким чином, Україна здатна за допомогою міжнародних партнерів посилювати свою інформаційну безпеку та захищати своє право на правдиве висвітлення подій. Прояви інформаційного тероризму в російсько-українській війні ще раз підтверджують важливість інформаційного контролю та боротьби з дезінформацією для забезпечення стабільності й суверенітету держави.

ВИСНОВКИ

Для сучасних конфліктів характерним є зростання проявів державного інформаційного тероризму. Це явище включає в себе використання інформаційних технологій і медіа для досягнення політичних, військових і психологічних цілей через маніпулювання громадською думкою, поширення фальшивих новин, кібератаки, а також психологічний тиск на населення і уряд. Інформаційний тероризм може бути набагато ефективнішим за традиційні методи агресії, оскільки він дозволяє впливати на маси без фізичного насильства і з меншими міжнародними наслідками.

Сучасні теоретичні підходи висвітлюють значний вплив інформаційного тероризму на перехід держав від традиційної форми ведення війни до гібридної. Інформаційний тероризм і традиційна війна проявляються у поєднанні військових та психологічних операцій. Інформаційні кампанії, зокрема через ЗМІ та соціальні мережі, супроводжують військові дії та створюють паніку серед населення, поширюючи недовіру до лідерів держави та змінюють наративи про конфлікт у міжнародному середовищі. Гібридний підхід несе в собі використання економічного тиску, пропаганди та маніпуляцій для дезорієнтації супротивника, а інформаційний тероризм стає інструментом впливу на різні аспекти національної безпеки, перетворюючи війну на багатoshаровий процес з менш вираженими межами між військовими та невійськовими методами.

Інформаційний тероризм став важливим інструментом у стратегії гібридної війни, особливо у контексті агресії росії проти України. Аналізуючи вплив росії на інфопростір України з часів її незалежності та до повномасштабного вторгнення, авторка дійшла наступних висновків. Ще з моменту набуття незалежності, Україна піддавалася постійному інформаційному впливу з боку росії. РФ активно використовувала медіа-ресурси, культурно-історичні наративи, а також проводила постійні пропагандистські кампанії для

формування залежного інфопростору України та створення політичних і соціальних розколів в середині держави. Порівнюючи терористичні прояви РФ проти України напередодні та під час повномасштабної агресії в Україні, варто зазначити, що до вторгнення акцент робився на інформаційній війні для просування проросійських наративів, які мали на меті підготувати підґрунтя для майбутніх виправдань щодо початку війни, а вже після вторгнення інформаційний терор посилювався та доповнювався класичним державним терором, спрямованим на знищення інфраструктури країни, залякування населення та підлив міжнародної підтримки України.

Одним з найбільш відомих прикладів використання інформаційного тероризму росією є «війна пам'яті», яка має на меті дискредитацію України як незалежної держави, а також послаблення її національної ідентичності. Росія активно використовує пропаганду, аби переконати українців у тому, що їхня національна ідентичність є штучною, а також пропагує радянські цінності як нібито єдину основу для об'єднання з росією. Це включає в себе масоване поширення інформації через телевізійні канали, соціальні мережі, новинні агентства, а також пропагандистські фільми та статті.

У період з 2014 року активізувалася спеціальна інформаційна війна росії. Наприклад, російські ЗМІ активно поширювали дезінформацію про українських військових, обвинувачуючи їх у злочинах проти цивільного населення, що мало на меті дестабілізувати ситуацію в Україні та підірвати довіру до уряду. Один з найбільш відомих прикладів — це фальшиві новини про так звану «кровожерливість» українських солдатів, що нібито вчиняють масові вбивства серед мирних мешканців. Інші фальшиві новини стосувалися вигаданих нападів на російських мирних громадян українськими силами.

Крім того, у рамках інформаційного тероризму росія активно використовує соціальні мережі для маніпуляції громадською думкою. Кібератаки, спрямовані на злам політичних партій, урядових установ, інформаційних агентств та приватних компаній, стали регулярним явищем під час конфлікту. Це дозволяє росії отримати доступ до важливої інформації, а також поширювати фальшиві

новини або маніпулювати реальністю. Зокрема, за допомогою дезінформації росія також спробувала послабити міжнародну реакцію на окупацію Криму. Ще одним прикладом використання інформаційного тероризму є операція з поширення неправдивої інформації про катастрофу рейсу МН17 у 2014 році, що мало на меті відвернути увагу від росії як головного винуватця трагедії, а також підірвати міжнародну підтримку України.

Отже, потенційні та реальні загрози від інформаційного тероризму рф для інформаційної безпеки України полягають в наступному: поширенні дезінформації та фейкових новин, маніпуляції суспільною думкою через соціальні мережі, підриві довіри до влади держави, створення інформаційного хаосу та паніки, а також в спробі легітимізувати окупацію та повномасштабну агресію на міжнародній арені.

Незважаючи на величезні зусилля росії та неспівставність потенціалів інформаційного впливу на громадську думку як всередині нашої держави, так і за кордоном, Україна активно відповідає на інформаційні атаки. Одним із кроків стало створення «Центру протидії дезінформації», метою якого є відстеження, спростування і боротьба з фальшивими новинами, що з'являються в інформаційному просторі.

На міжнародному рівні Україна намагається мобілізувати підтримку від міжнародних партнерів, таких як Європейський Союз і НАТО, щодо посилення санкцій проти росії за її інформаційні та терористичні атаки. В Україні активно розвиваються ініціативи, спрямовані на підвищення медіаграмотності населення. Це включає в себе освітні програми, які навчають громадян, як виявляти фальшиві новини, а також як бути більш критичними щодо отримуваної інформації.

Підсумовуючи, необхідно зауважити, що інформаційний тероризм росії проти України є складним і багатоетапним процесом, що включає в себе поширення дезінформації, кібератаки та психологічні операції. Він є важливою частиною гібридної війни, яка ведеться росією не тільки на політичному, а й на інформаційному фронті. Протидія таким атакам потребує не лише внутрішніх

зусиль України, а й міжнародної кооперації для забезпечення інформаційної безпеки та стабільності в регіоні.

Це показує, що в умовах сучасних конфліктів інформаційна складова є таким же важливим аспектом, як і військова сила. Протидія інформаційному тероризму вимагає від держави комплексного підходу, здатності швидко реагувати на нові загрози та залучення всіх можливих ресурсів для захисту національних інтересів. Враховуючи активне використання інформації в сучасних конфліктах та перехід від класичної війни до гібридної, перспективи запровадження санкцій стають все більше реалістичними, оскільки як держави, так і міжнародні організації визнають загрози, які несуть методи інформаційного тероризму. Варто очікувати, що в майбутньому міжнародна спільнота створить чіткі закони, які будуть регулювати інформаційний простір, а також запобігати проявам інформаційного тероризму.

СПИСОК ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Білічак О., Гуз А. Гібридна війна як інструмент зовнішньої політики російської федерації: український вимір (1991–2023). *Східноєвропейський історичний вісник*. 2024. № 30. С. 162–178. URL: <https://doi.org/10.24919/2519-058x.30.299897> (Дата звернення: 10.11.2024).
2. Борщ як частина українського культурного коду. *Ukrainer*. URL: <https://www.ukrainer.net/borshch/> (Дата звернення: 10.11.2024).
3. Британія та Туреччина скупили українське зерно. *DisinfoChronicle*. *Кремлівська дезінформація щодо військового наступу на Україну - Детектор медіа*. 12.02.2022. URL: <https://disinfo.detector.media/post/velyka-brytaniia-ta-turechchyna-planuiut-skupyty-ukrainske-zerno-i-pryrekty-ukrainu-na-holod> (Дата звернення: 10.11.2024).
4. Відео з обезголовленням українських воїнів окупантами: що відомо та яка реакція влади. *Texty.org.ua*. URL: <https://texty.org.ua/fragments/109402/video-z-obezholovlenniam-ukrayinskyh-voyini-v-okupantamy-sho-vidomo-ta-yaka-reaksiya-vlady/> (Дата звернення: 09.11.2024).
5. Декодування проросійських інформаційних стратегій у Центрально-Східній Європі: січень 2024. *Детектор медіа*. URL: https://detector.media/propahanda_vplyvy/article/225172/2024-04-08-dekoduвання-prorosiyskykh-informatsiynykh-strategiy-u-tsentralno-skhidniy-ievropi-sichen-2024-go/ (Дата звернення: 10.11.2024).
6. Детектор медіа. URL: <https://detector.media/>.
7. Заборона пов'язаних з РФ релігійних організацій: Рада заперечує зволікання із показом законопроекту. *Укрінформ*. 03.05.2024. URL: <https://www.ukrinform.ua/rubric-society/3859508-zaborona-povazanih-z-rf-religijnih-organizacij-u-radi-zaperecuut-zvolikanna-iz-opriludnennam-zakonoproektu.html> (Дата звернення: 10.11.2024).
8. Запорізька АЕС: захоплення окупантами, ядерний тероризм. *Міністерство внутрішніх справ*. URL:

<https://mvs.gov.ua/news/zaporizka-aes-zaxoplennia-okupantami-iadernii-terorizm>
(Дата звернення: 09.11.2024).

9. «Захист Батьківщини — кара», «партія ухилянтів перемогла би “Слугу народу”». Тези російської пропаганди щодо мобілізації в Україні / Л. Бідочко. *ms.detector.media*. 18.04.2024. URL: <https://ms.detector.media/propaganda-ta-vplivi/post/34703/2024-04-18-zakhyst-batki-vshchyny-kara-partiya-ukhylyantiv-peremogla-by-slugu-narodu-tezy-rosiyskoi-propagandy-shchodo-mobilizatsii-v-ukraini/> (Дата звернення: 11.11.2024).

10. Збій в енергосистемі України був викликаний кібератакою - SANS ICS. *New Voice*. 10.01.2016. URL: <https://nv.ua/ukr/ukraine/events/zbij-v-energosissemi-ukrajini-buv-viklikanij-kiberatakoju-sans-ics-90274.html>. (Дата звернення: 09.11.2024).

11. Карлашук В. У Києві викрили групу, яка ошукала 5 тисяч постраждалих від війни людей на 100 мільйонів гривень. *Суспільне Київ*. 29.06.2022. URL: <https://suspilne.media/kyiv/255165-u-kievi-vikrili-grupu-aka-osukala-5-tisac-postrazdahih-vid-vijni-ludej-na-100-miljoniv-griven/> (Дата звернення: 08.11.2024).

12. Касем Сулеймані: чому США вбили його саме зараз. *BBC News Україна*. 03.01.2020. URL: <https://www.bbc.com/ukrainian/features-50985226> (Дата звернення: 09.11.2024).

13. Команда «каналів Медведчука» розпочала мовлення на Першому незалежному. *Детектор media*. 26.02.2021. URL: <https://detector.media/rinok/article/185302/2021-02-26-komanda-kanaliv-medvedchuka-rozpochala-movlennya-na-pershomu-nezaleznomu/> (Дата звернення: 09.11.2024).

14. Конвенція про заборону застосування, накопичення запасів, виробництва і передачі протипіхотних мін та про їхнє знищення (укр/рос): Конвенція Організація Об'єднаних Націй від 18.09.1997 р. (станом на 18 трав. 2005 р.). *База даних «Законодавство України»*. URL: https://zakon.rada.gov.ua/laws/show/995_379#Text (Дата звернення: 10.11.2024).

15. Конвенція про захист цивільного населення під час війни (укр/рос): Конвенція Організація Об'єднаних Націй від 12.08.1949. *База даних «Законодавство України»*. URL: https://zakon.rada.gov.ua/laws/show/995_154#Text (Дата звернення: 10.11.2024).
16. Коновальчук П. І. Зміст та основні напрями пропаганди російської православної церкви у контексті гібридної війни Росії проти України. *Стратегічна панорама*. 2018. № 2. С. 31–36.
17. Конфлікт у Нагірному Карабасі: з чого все почалося. *Chas News*. 25.09.2023. URL: <https://chas.news/current/konflikt-mizh-azerbaidzhanom-ta-virmeniyu-poyasnyuem-o-chomu-kraini-voroguuyut-cherez-nagirnii-karabah> (Дата звернення: 03.11.2024).
18. Короп І. Інформаційний тероризм. *Альманах міжнародного права*. 2017. № 18. С. 96–102. URL: <http://www.inlawalmanac.mgu.od.ua/v18/14.pdf> (Дата звернення: 02.11.2024).
19. Кравчук А. Феномен «розіп'ятого хлопчика». Як працює російська пропаганда та що за техніка «60/40». *OBOZREVATEL NEWS*. 01.06.2022. URL: <https://news.obozrevatel.com/ukr/lady/psychology/fenomen-rozipyatogo-hlopchika-yak-pratsyue-rosijska-propaganda-ta-scho-za-tehnika-6040.htm> (Дата звернення: 10.11.2024).
20. Крижний А. Кібератака української розвідки паралізувала банківську та платіжну системи РФ. *Економічна правда*. 24.07.2024. URL: <https://www.epravda.com.ua/news/2024/07/24/717061/> (Дата звернення: 14.10.2024).
21. Леонов Б., Лихова С. Інформаційний тероризм як загроза національній безпеці України. *Scientific works of national aviation university. series: law journal "Air and space law"*. 2021. Т.2, №59. С. 170–176. URL: <https://doi.org/10.18372/2307-9061.59.15615> (Дата звернення: 14.10.2024).
22. Магда Є. Гібридна війна: вижити і перемогти. Харків: Vivat, 2015. 304 с.

23. Медіаграмотність як ключ до боротьби з російською пропагандою: виклики та рішення для України. *Центр стратегічних комунікацій*. URL: <https://spravdi.gov.ua/mediagramotnist-yak-klyuch-do-borotby-z-rosijskoyu-propagandoyu-vyklyky-ta-rishennya-dlya-ukrayiny/>.

24. Міністерство культури та стратегічних комунікацій України. URL: <https://mesc.gov.ua/>

25. Московський патріарх Кирил заявив у проповіді, що росія «ніколи ні на кого не нападала». *Укрінформ*. 04.05.2022. URL: <https://www.ukrinform.ua/rubric-world/3474354-moskovskij-patriarh-kiril-zaaviv-u-propovidi-so-rosia-nikoli-ni-na-kogo-ne-napadala.html> (Дата звернення: 10.11.2024).

26. ОЗХЗ встановила застосування хлору в квітні в Думі. *Радіо Свобода*. 06.07.2018. URL: <https://www.radiosvoboda.org/a/news/29347741.html> (Дата звернення: 10.11.2024).

27. Окупація Криму Росією: шість років тому “зелені чоловічки” прийшли на півострів. *Укрінформ*. 20.02.2020 URL: <https://www.ukrinform.ua/rubric-crimea/2880169-okupacia-krimu-rosieu-sist-rokiv-tomu-zeleni-colovicki-prijsli-na-pivostriv.html> (Дата звернення: 11.11.2024).

28. Олексій Кустовський : Facebook-сторінка. *Facebook*. URL: <https://www.facebook.com/photo.php?fbid=1781894558546262&set=a.364125046989894&type=3&mibextid=WaXdOe>

29. Про внесення змін до деяких законодавчих актів України щодо заборони політичних партій: Закон України від 03.05.2022 № 2243-IX. *База даних «Законодавство України»*. URL: <https://zakon.rada.gov.ua/laws/show/2243-20#Text> (Дата звернення: 11.11.2024).

30. Про забезпечення функціонування української мови як державної: Закон України від 25.04.2019 № 2704-VIII: станом на 27 черв. 2024 р. *База даних «Законодавство України»*. URL: <https://zakon.rada.gov.ua/laws/show/2704-19#Text> (Дата звернення: 09.11.2024).

31. Про захист конституційного ладу у сфері діяльності релігійних організацій: Закон України від 20.08.2024 р. № 3894-IX. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/3894-20#Text> (Дата звернення: 13.11.2024).

32. Про створення Центру протидії дезінформації: Рішення Ради національної безпеки і оборони України від 11.03.2021 р. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/n0015525-21#Text> (Дата звернення: 13.11.2024).

33. Протести в Іраку: кількість загиблих зросла до 340 людей. Радіо Свобода. 23.11.2019. URL: <https://www.radiosvoboda.org/a/news-protesty-v-iraku-340-zahyblyh/30288127.html> (Дата звернення: 10.11.2024).

34. Протокол про вибухонебезпечні предмети - наслідки війни: Протокол Організація Об'єднаних Націй від 28.11.2003 р. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/995_c78#Text (Дата звернення: 10.11.2024).

35. Російські військові розстрілюють людей зі зв'язаними руками. Віртуальний музей російської пропаганди. 04.03.2022. URL: <https://rusaggression.gov.ua/ua/masovi-vbyvstva-v-buchia3334551b9ba685852652000de021148.html> (Дата звернення: 11.11.2024).

36. Російська пропаганда. Центр стратегічних комунікацій. URL: <https://spravdi.gov.ua/rosijska-propaganda/>

37. Росія торік витратила на пропаганду у медіа \$1,9 мільярда. Укрінформ. 19.05.2023. URL: <https://www.ukrinform.ua/rubric-world/3711327-rosia-torik-vitratila-na-propagandu-u-media-19-milarda.html> (Дата звернення: 14.10.2024).

38. Скільки грошей росія витрачає на фінансування державної пропаганди. Слово і діло. 10.10.2024. URL:

<https://www.slovoidilo.ua/2024/10/10/infografika/finansy/skilky-hroshej-rosiya-vytrachaye-finansuvannya-derzhavnoyi-propahandy>

39. Скляревська Г. Чому «Азов» – не «неонацистський батальйон». *Детектор медіа*. 01.06.2022. URL: <https://ms.detector.media/propaganda-ta-vplivi/post/29596/2022-06-01-chomu-azov-ne-neonatsystskyu-batalyon/> (Дата звернення: 10.11.2024).

40. Служба Безпеки України. Підозра патріарху РПЦ Кирилу. *Офіційний Telegram-канал*. URL: <https://t.me/SBUkr/10248> (Дата звернення: 03.11.2024).

41. Тараненко В. У Бучі в братських могилах похоронено 287 мирних людей, яких вбили російські окупанти. *ГЛАВКОМ*. 03.04.2022. URL: <https://glavcom.ua/news/u-buchi-v-bratskih-mogilah-pohoroneno-287-mirnih-lyudey-yakih-vbili-rosiyski-okupanti-835111.html> (Дата звернення: 14.11.2024).

42. Трамп оголосив про вихід США з ядерної угоди з Іраном - BBC News Україна. *BBC News Україна*. 08.05.2018. URL: <https://www.bbc.com/ukrainian/news-44044107> (Дата звернення: 14.11.2024).

43. Українці стали частіше користуватися інтернетом, 80% – онлайн щодня: соціопитування. *UNDP*. 26.01.2024. URL: <https://www.undp.org/uk/ukraine/press-releases/ukrayintsi-staly-chastishe-korystuvatysya-internetom-80-onlayn-shchodnya-sotsopytuvannya> (Дата звернення: 14.10.2024).

44. ФЕЙК: Знайдений шолом льотчика НАТО – доказ участі Альянсу в бойових діях в Україні. *VoxUkraine*. 27.07.2022. URL: <https://voxukraine.org/fejk-znajdenyj-sholom-lotchyka-nato-dokaz-uchasti-alyansu-v-bojovyh-diyah-v-ukrayini> (Дата звернення: 09.11.2024).

45. «Фортеця Львів» – чергова російська ІПСО. *АрміяInform*. 19.08.2023. URL: <https://armyinform.com.ua/2023/08/19/forteczya-lviv-cherгова-rosijska-ipso/> (Дата звернення: 09.11.2024).

46. Хакери зламали сервери студії Sony і злили в мережу кілька нових фільмів. *LB.ua*. 01.12.2014. URL:

https://lb.ua/culture/2014/12/01/287858_hakeri_vzломali_servera_studii_sony.html
(Дата звернення: 14.11.2024).

47. Харченко І. О. Боротьба України з російським інформаційним тероризмом в умовах війни. *Крим та Чорноморський регіон: реконструктивний розвиток у воєнний та повоєнний період*: матеріали Міжнародної науково-практичної конференції Таврійського національного університету імені В. І. Вернадського, м. Київ, 17–18 жовт. 2024 р. 2024.

48. Чому Буча стала символом майбутньої перемоги. *Центр протидії дезінформації*. 31.03.2023. URL: <https://cpd.gov.ua/articles/chomu-bucha-stala-symvolom-majbutnoyi-peremogy/>
(Дата звернення: 14.11.2024).

49. Шутняк Л. Як Україна воює з Росією на інформаційному фронті. *Explainer*. 23.05.2024. URL: <https://explainer.ua/bitva-za-gromadsku-dumku-yak-ukrayina-voyuye-z-rosiyeyu-na-informatsijnomu-fronti/> (Дата звернення: 18.11.2024).

50. 100 брехливих російських наративів про російсько-українську війну. Збірник інформаційно-аналітичних матеріалів /А. М. Романишин та ін. Київ: НДЦ ГП ЗС України, 2023. 77 с.

51. Aliaksandrau A. Brave new war: The information war between Russia and Ukraine. *Index on Censorship*. 2014. Vol. 43, no. 4. P. 54–60. URL: <https://doi.org/10.1177/0306422014560963> (Last access: 14.11.2024).

52. Anwar K. Russia-China's Information Warfare In A Changing Global Order. *TDHJ.org*. Nov. 28, 2022. URL: <https://tdhj.org/blog/post/russia-china-information-warfare-changing-global-order/> (Last access: 15.11.2024).

53. Arquilla J., Ronfeldt D., Zanini M. Information-Age Terrorism. *Current History*. 2000. Vol. 99, no. 636. P. 179–185. URL: <https://doi.org/10.1525/curh.2000.99.636.179> (Last access: 15.11.2024).

54. Barseghyan A. Pashinyan suggests Russia used Nagorno-Karabakh as ‘a leash’ on Armenia. *OC Media*. 11.04.2024. URL:

<https://oc-media.org/pashinyan-suggests-russia-used-nagorno-karabakh-as-a-leash-on-armenia/> (Last access: 03.11.2024).

55. Benkler Y. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. New York, US: Oxford University Press, 2018. 472 p. URL: <http://surl.li/ypnpne>. (Last access: 03.11.2024).

56. Bernays E. L. *Propaganda*. New York: H. Liveright, 1928. 159 p. URL: https://www.voltairenet.org/IMG/pdf/Bernays_Propaganda_in_english_.pdf (Last access: 01.11.2024).

57. Bond S. Facebook takes down Russian network impersonating European news outlets. *NPR*. 27.09.2022. URL: <https://www.npr.org/2022/09/27/1125217316/facebook-takes-down-russian-network-impersonating-european-news-outlets> (Last access: 09.11.2024).

58. Borch O. J., Heier T. *Preparing for Hybrid Threats to Security*. London : Routledge, 2024. 312 p. URL: <https://doi.org/10.4324/9781032617916> (Last access: 18.11.2024).

59. Brovko L. The culmination of Russia's special operation "Maidan 3" against Ukraine will happen in the spring. *Бабель*. 27.02.2024. URL: <https://babel.ua/en/news/104353-the-culmination-of-russia-s-special-operation-maidan-3-against-ukraine-will-happen-in-the-spring> (Дата звернення: 03.11.2024).

60. Brown S. In Russia-Ukraine war, social media stokes ingenuity, disinformation. *MIT Management Sloan School*. URL: <https://mitsloan.mit.edu/ideas-made-to-matter/russia-ukraine-war-social-media-stokes-ingenuity-disinformation> (Last access: 15.11.2024).

61. Buzan B., Wæver O., de Wilde J. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, 1998. 239 p.

62. Conflict Between Turkey and Armed Kurdish Groups. *Global Conflict Tracker*. URL: <https://www.cfr.org/global-conflict-tracker/conflict/conflict-between-turkey-and-armed-kurdish-groups> (Last access: 15.11.2024).

63. Cyber Operations during the Russo-Ukrainian War / G. B. Mueller et al. *CSIS*. 13.07.2023. URL: <https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war#h2-conclusion> (Last access: 03.11.2024).
64. Danyk Y., Maliarchuk T., Briggs C. Security Aspects of Hybrid War, COVID-19 Pandemic and Cyber-Social Vulnerabilities. *Connections QJ* 20. June, 2021. No. 3. P. 45-70. URL: https://www.researchgate.net/publication/371634161_Security_Aspects_of_Hybrid_War_COVID-19_Pandemic_and_Cyber-Social_Vulnerabilities (Last access: 15.11.2024).
65. Entman R. M. Framing: Toward Clarification of a Fractured Paradigm. *Journal of Communication*. 1993. Vol. 43, no. 4. P. 51–58. URL: <https://doi.org/10.1111/j.1460-2466.1993.tb01304.x> (Last access: 12.11.2024).
66. Entous A., Schmitt E., Barnes J. E. Biden Allows Ukraine to Strike Russia With Long-Range U.S. Missiles. *The New York Times*. Nov. 17, 2024. URL: <https://www.nytimes.com/2024/11/17/us/politics/biden-ukraine-russia-atacms-missiles.html> (Last access: 17.11.2024).
67. Giles K. Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power: Research Paper. Chatham House, the Royal Institute of International Affairs. 2016. 73 p. URL: <https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf>.
68. Hague Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land: of 18.10.1907. URL: <https://www.refworld.org/legal/agreements/hague/1907/en/31788> (Last access: 03.11.2024).
69. Hanson R., Grissom A. R., Mouton C. A. The Future of Indo-Pacific Information Warfare Challenges and Prospects from the Rise of AI. *RAND*. Mar. 14, 2024. URL: https://www.rand.org/pubs/research_reports/RRA2205-1.html (Last access: 02.11.2024).

70. Hassan M. ISIS and the Assad regime: Strategy and counter-strategy in Syria's Badia. *Middle East Institute*. URL: <https://www.mei.edu/publications/isis-and-assad-regime-strategy-and-counter-strategy-syrias-badia> (Last access: 12.11.2024).
71. Herman E. S., Chomsky N. Manufacturing consent: The political economy of the mass media. London: Bodley Head, 2008. 582 p. URL: <http://surl.li/clmqfb> (Last access: 25.10.2024).
72. Hlushchuk Y. Fakes as a Tool of Pressure in War Conditions: Specifics of Application and Perception. *Naukovì praci Nacional'noi biblioteki Ukraïni ìmenì V Ì Vernads'kogo*. 2023. No. 67. P. 96–107. URL: <https://doi.org/10.15407/np.67.096> (Last access: 12.11.2024).
73. Hoffman F. G. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, Virginia: Potomac Institute for Policy Studies, 2007. URL: https://www.potomac institute.org/images/stories/publications/potomac_hybridwar_0108.pdf (Last access: 02.11.2024).
74. Hordiichuk O., Halapsis A., Kozlovets M. How the Information Warfare Turns Into Full-Scale Military Agression: the Experience of Ukraine. *Przegląd Strategiczny*. 2024. No. 16. P. 345–362. URL: <https://doi.org/10.14746/ps.2023.1.25> (Last access: 18.11.2024).
75. Hoskins A., Tulloch J. Print Media and the Climax of the Global Financial Crisis. *Risk and Hyperconnectivity*. 2016. P. 52–87. URL: <https://doi.org/10.1093/acprof:oso/9780199375493.003.0003> (Last access: 12.11.2024).
76. Hybrid threats: Reconceptualizing the evolving character of modern conflict / ed. by National Defense University. Institute for National Strategic Studies. Washington, D.C.]: Institute for National Strategic Studies, National Defense University. April 2009. No.240. 8 p. URL: <https://www.files.ethz.ch/isn/98862/SF240.pdf>.
77. Jacek D. AQAP Inspire Magazine as a tool motivating to terrorist activities. *Przegląd Bezpieczeństwa Wewnętrznego*. 2019. Vol. 11, no. 20. P. 339–352.

URL: <https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-ece248ec-620e-476a-8473-41ed81d574a0> (Last access: 26.10.2024).

78. Kilcullen D. *Out of the Mountains: The Coming Age of the Urban Guerrilla*. Oxford University Press, Incorporated, 2013. 353 p.

79. LachenBots : Telegram-канал. *Telegram*. URL: <https://t.me/lachenbots>

80. Lang J. Antipode Acquires Tallinn Competition Anti-War Film 'Deaf Lovers,' Pulled From Fest's Ukrainian Section (EXCLUSIVE). *Variety*. Nov. 17, 2024 URL: <https://variety.com/2024/film/global/antipode-acquires-deaf-lovers-boris-guts-tallinn-1236212495/> (Last access: 03.11.2024).

81. Leonardson J. E. Intelligence in Public Media. *Studies in Intelligence*. 2020. Vol. 64, no. 1. 5 p. URL: <https://www.cia.gov/resources/csi/static/active-measures-and-information-wars.pdf> (Last access: 06.11.2024).

82. Lewis J. A. Cyber War and Ukraine. *CSIS*. June 2022. 14 p. URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220616_Lewis_Cyber_War.pdf?VersionId=S.iEKeom79InugnYWlcZL4r3Ljuq.ash (Last access: 02.11.2024).

83. Libicki M. C. *Cyberdeterrence and Cyberwar*. RAND Corporation, 2009. 239 p.

84. Lysko T. D., Klimuk O. O., Lysianska D. V. Information terrorism as a threat to national security and a method of information warfare. *Juridical scientific and electronic journal*. 2022. No. 10. P. 574–576. URL: <https://doi.org/10.32782/2524-0374/2022-10/143> (Last access: 01.11.2024).

85. McChesney R. W. *Digital Disconnect: How Capitalism Is Turning the Internet Against Democracy*. New Press, 2013. URL: https://books.google.com.ua/books?id=j_7EkTI8kVQC&pg=PA96&hl=ru&source=gbv_toc_r&cad=2#v=onepage&q&f=false (Last access: 10.10.2024).

86. Miller C., Reffin J. IstandwithRussia - Anatomy of a Pro-Kremlin Influence Operation. *ISD*. March 2022. URL: https://www.isdglobal.org/digital_dispatches/istandwithrussia-anatomy-of-a-pro-kremlin-influence-operation/ (Last access: 08.11.2024).
87. O'Donnell V. J., Jowett G. S. Propaganda and Persuasion - Chapter 1. 4th ed. SAGE Publications, Incorporated, 2005. 48 p.
88. Paterson T., Hanley L. Political warfare in the digital age: cyber subversion, information operations and 'deep fakes'. *Australian Journal of International Affairs*. 2020. Vol. 74, no. 4. P. 439–454. URL: <https://doi.org/10.1080/10357718.2020.1734772> (Last access: 18.11.2024).
89. Patlashynska I. V. Modern Russian-Ukrainian information war: tasks, methods and features of use. *Scientific Journal "Regional Studies"*. 2022. No. 28. P. 84–87. URL: <https://doi.org/10.32782/2663-6170/2022.28.15> (Last access: 18.11.2024).
90. Paul C., Matthews M. The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It. *RAND Corporation*. 2016. URL: <https://doi.org/10.7249/pe198> (Last access: 09.11.2024).
91. Rovner J. Cyber War as an Intelligence Contest - War on the Rocks. *War on the Rocks*. September 2019. URL: <https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/> (Last access: 02.11.2024).
92. Russia is swaying Twitter users outside the West to its side. *The Economist*. 14.05.2022. URL: <https://www.economist.com/graphic-detail/2022/05/14/russia-is-swaying-twitter-users-outside-the-west-to-its-side> (Last access: 03.11.2024).
93. Shuya M. Russian Cyber Aggression and the New Cold War. *Journal of Strategic Security*. 2018. Vol. 11, no. 1. P. 1–18. URL: <https://doi.org/10.5038/1944-0472.11.1.1646> (Last access: 18.11.2024).
94. Syria and Russia have long used disinformation to deflect attention from appalling war crimes committed by the Assad regime: Statement by Fergus

Eckersley, UK Political Coordinator at the UN, at the UN Security Council briefing on chemical weapons in Syria. *GOV.UK*. 25.10.2022. URL: <https://www.gov.uk/government/speeches/syria-and-russia-have-long-used-disinformation-to-deflect-attention-from-appalling-war-crimes-committed-by-the-assad-regime> (Last access: 09.11.2024).

95. The Analysis of World Information Warfare and Information Security in the Context of the Russian-Ukrainian War / S. Lysenko et al. *Studies in Media and Communication*. 2023. Vol. 11, no. 7. P. 150-158. URL: <https://doi.org/10.11114/smc.v11i7.6414> (Last access: 09.11.2024).

96. UA War Infographics: Telegram-канал. *Telegram*. URL: <https://t.me/uawarinfographics/515>

97. Ukraine and Beyond / ed. by J. H. Matlary, T. Heier. Cham: Springer International Publishing, 2016. URL: <https://doi.org/10.1007/978-3-319-32530-9> (Last access: 18.11.2024).

98. Warsaw Summit Communiqué issued by NATO Heads of State and Government (Official text). NATO. 09.07.2016. URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en (Last access: 02.11.2024).

99. Zadorožna M., Butuc M. Russian disinformation in Moldova and Poland in the context of the Russo-Ukrainian war. *Security and Defence Quarterly*. 2024. Vol. 46, no. 2. P. 47–65. URL: <https://doi.org/10.35467/sdq/189686> (Last access: 09.11.2024).

100. Zhalimas D. Russian justification of the annexation of Crimea and Nazi Propaganda: great similarities and minor differences. *Ukrainian Journal of Constitutional Law*. 2017. Vol. 2. P. 17–29. URL: <https://doi.org/10.30970/jcl.2.2017.2> (Last access: 09.11.2024).

ДОДАТКИ

Додаток А. Приклади постерів у соціальних мережах

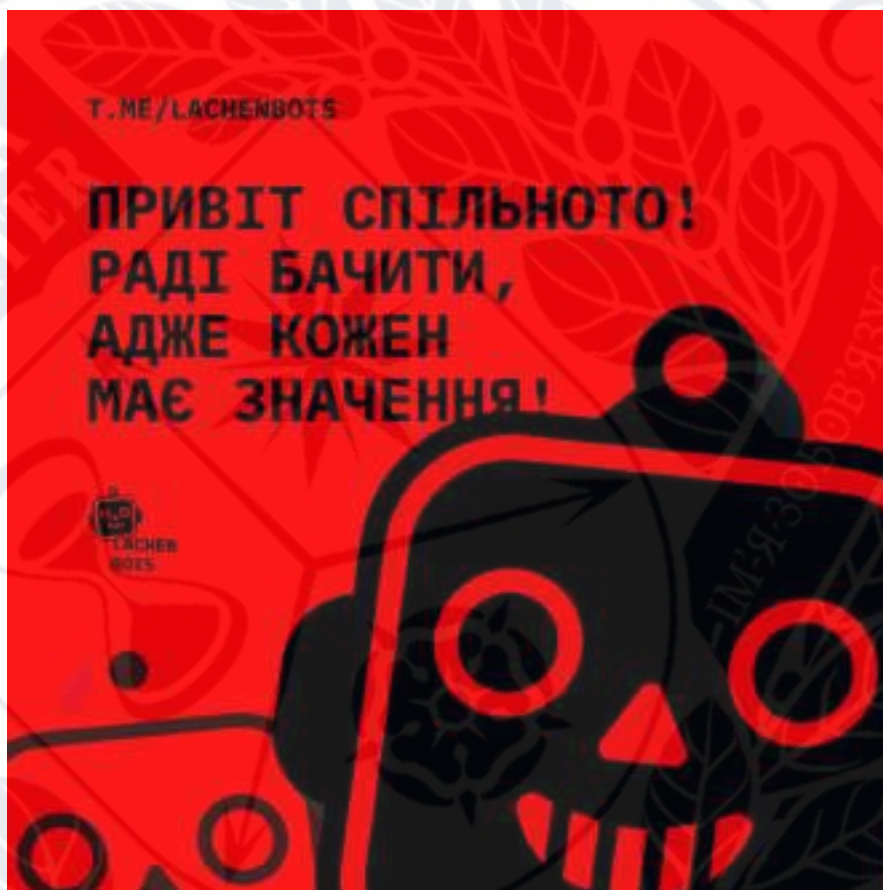


Рисунок А.1. - офіційний постер створеного Telegram-каналу, для боротьби з російською пропагандою¹

¹ Фото взяте з офіційного Телеграм каналу LachenBots URL: <https://t.me/lachenbots>

Додаток Б. Політичні карикатури Олексія Кустовського



Рисунок Б.1. – карикатура про значення отриманого Томасу для України²



Рисунок Б.2. – карикатура із зображенням поширення російської пропаганди³

² Карикатура взята з Facebook сторінки Олексія Кустовського URL: <https://www.facebook.com/photo.php?fbid=1781894558546262&set=a.364125046989894&type=3&mibextid=WaXdO>

³ Карикатура використана з сайту новин «Радіо свобода» URL: <https://www.radiosvoboda.org/a/27551780.html>

Додаток В. Офіційні постери кінострічок та мюзиклу



Рисунок В.1. – біографічна драма «Заборонений»



Рисунок В.2. – документальний військовий фільм «20 днів в Маріуполі»



Рисунок В.3. – історична драма «Щедрик»



Рисунок В.4. – український містичний фільм жахів «Конотопська відьма»

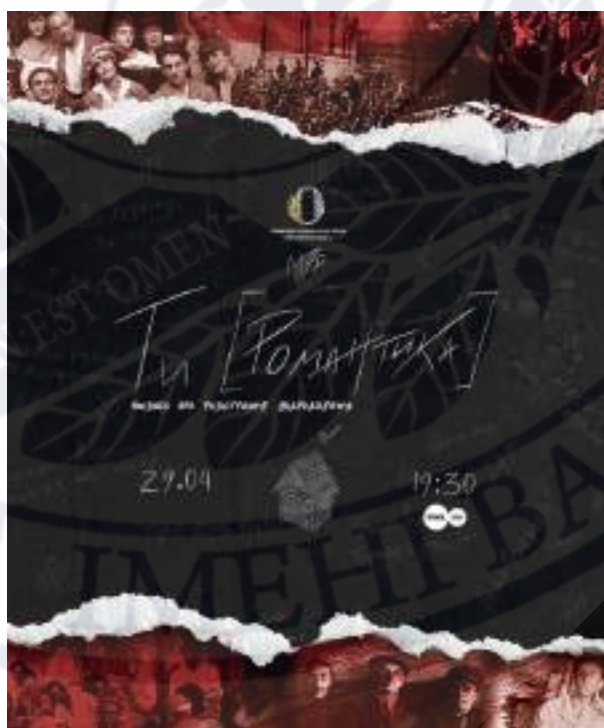


Рисунок В.5. – Реп-мюзикл "Ти [Романтика]"

Додаток Г. Візуальні матеріали, що ілюструють російський інформаційний тероризм і пропаганду



Рисунок Г.1. - витрати рф на поширення пропаганди під час російсько-української війни⁴

⁴ Бюджет російської пропаганди. Слово і діло URL: <https://www.slovoidilo.ua/2024/10/10/infografika/finansy/skilky-hroshej-rosiya-vytrachaye-finansuvannya-derzhavnyi-propahandy>



Рисунок Г.2. - кількість російських вкидів в інфопростір з моменту повномасштабного вторгнення⁵

⁵

Графіка створена «Детектор медіа». URL: <https://detector.media/monitorynh-internetu/article/234651/2024-11-13-ukrainskyy-svyashchennyk-nazvav-trampa-anty-khrystom-oglyad-rosiyskoi-dezinformatsii-za-410-lystopada-2024-roku/>

Similarity diagram of accounts tweeting pro-Russian hashtags*
March 7th-9th 2022

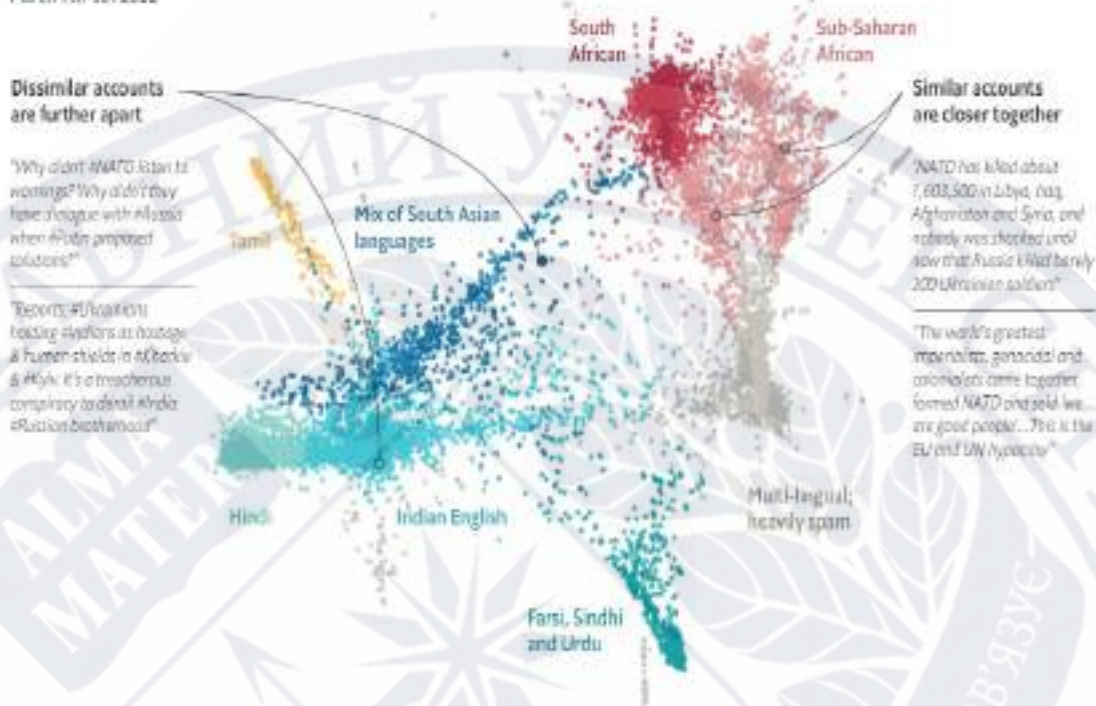


Рисунок Г.3. – вплив російської пропаганди на соціальні мережі в Азії та Африці⁶

⁶ Дані взято з Телеграм каналу «UA War Infographics» URL: <https://t.me/uawarinfolgraphics/515>



Рисунок Г.4. – графік кількості кібератак росії протягом 2021 – 2023 років⁷

⁷ Дані взято з Телеграм каналу «UA War Infographics» URL: <https://t.me/uawarininfographics/2970>

РОСІЙСЬКІ КІБЕРАТАКИ НА СІЛЬСЬКЕ ГОСПОДАРСТВО УКРАЇНИ

TOP
LEAD

росія атакувала українську аграрну інфраструктуру не лише ракетами, вона одночасно залучала до атак пропагандистів та хакерів.

Етапи російських атак на об'єкти аграрної інфраструктури України, липень-серпень 2023



t.me/uawarinfographics

Рисунок Г.5. – етапи російських атак на об'єкти аграрної інфраструктури України, липень-серпень 2023 року⁸

⁸ Дані взято з Телеграм каналу «UA War Infographics» URL: <https://t.me/uawarinfographics/3070>

Динаміка публікацій про Україну у січні 2024

В Болгарії, Молдові, Польщі, Румунії,
Словаччині, Угорщині, Україні і Чеській
Республіці



Детектор медіа за даними LetsData. Дані
включають такі соціальні мережі:
Facebook, Telegram, Twitter і YouTube

детектор медіа

Рисунок Г.6. – динаміка публікацій про Україну в січні 2024 року в країнах ЦСЄ⁹

⁹ Дані взято з дослідження «Детектора медіа» URL: https://detector.media/propahanda_vplyvy/article/225172/2024-04-08-dekoduvannya-prorosyiskykh-informatsiynykh-strategiy-u-tsentralno-skhidny-ievropi-sichen-2024-go/