

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ**

ГУМАНІТАРНО-ПЕДАГОГІЧНИЙ ФАКУЛЬТЕТ

УДК 327:341.43(4) «20»

ПОГОДЖЕНО
Декан факультету (Директор ННІ)
гуманітарно-педагогічного факультету,
кандидат філософських наук, доцент

_____ Савицька І.М.
« ____ » _____ 2024 р.

ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ
В.о. Завідувача кафедри
міжнародних відносин і суспільних
наук, кандидат історичних наук,
доцент

_____ Хвіст В.О.
« ____ » _____ 2024 р.

МАГІСТЕРСЬКА РОБОТА

на тему:

**Інформаційна війна як перманентний процес світової політики:
ініціатори і жертви інформаційної війни**

**Information war as a permanent process of world politics: initiators and
victims of information**

Спеціальність: Міжнародні відносини, суспільні комунікації та регіональні студії

Магістерська програма: Міжнародні відносини, суспільні комунікації та регіональні студії

Програма підготовки: освітньо-професійна

Гарант освітньої програми

_____ кандидат історичних наук, доцент Кравченко Н.Б.

Керівник магістерської роботи

кандидат історичних наук, доцент _____ Шевченко Н.В.

Виконала

_____ Осіюк І. Ю.

КИЇВ-2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ГУМАНІТАРНО-ПЕДАГОГІЧНИЙ ФАКУЛЬТЕТ

“ЗАТВЕРДЖУЮ”

**В.о. завідувача кафедри
міжнародних відносин і суспільних
наук**

_____ Хвіст В.О.

«___»_____ 2024 р.

ЗАВДАННЯ

ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ

СТУДЕНТУ

Осіюк Ірина Юріївна

**Спеціальність 291 «Міжнародні відносини, суспільні комунікації та
регіональні студії»**

**Освітня програма «Міжнародні відносини, суспільні комунікації та
регіональні студії»**

Орієнтація освітньої програми освітньо-професійна

**Тема магістерської роботи: «Інформаційна війна як перманентний процес
світової політики: ініціатори і жертви інформаційної війни»**

Затверджена наказом ректора НУБіП України від 10.02.2023.

Термін подання завершеної роботи на кафедру “ ___ ” _____ 2024

Вихідні дані до магістерської роботи:

- 1) Наукові дослідження з питань інформаційної війни та інформаційної агресії у XXI ст.;
- 2) Правові документи, що регламентують інформаційну безпеку та заходи протидії інформаційній агресії;
- 3) Вітчизняна та зарубіжна література, а також джерела інформації, що стосуються проблеми інформаційної війни та її впливу на суспільство.

Перелік питань, що підлягають дослідженню:

1. визначити термін «інформаційна війна» у сучасному науковому дискурсі та українському законодавстві;
2. проаналізувати основні підходи до дослідження інформаційної агресії та класифікацію інформаційних конфліктів;
3. розглянути особливості еволюції інформаційної війни в історичному контексті та її розвиток у Новий час;
4. висвітлити вплив новітніх інформаційних технологій, зокрема Інтернету та соціальних мереж, на сучасні інформаційні конфлікти;
5. охарактеризувати методи інформаційної агресії проти України та її особливості у порівнянні з іншими інформаційними конфліктами;
6. дослідити ініціаторів та інструменти, що застосовуються в інформаційній агресії проти України;
7. оцінити соціально-політичні наслідки інформаційної війни для українського суспільства;
8. визначити ефективність заходів протидії інформаційній агресії в Україні;

9. оцінити перспективи розвитку заходів протидії інформаційній агресії з урахуванням міжнародного досвіду;
10. дослідити можливості інтеграції міжнародних стратегій для зміцнення захисту України від інформаційної агресії.

Дата видачі завдання

“ ___ ” _____ 2024

Керівник магістерської роботи

_____ Шевченко Н.В.

Завдання прийняв до виконання

_____ Осіюк І. Ю.

Магістерська робота присвячена аналізу інформаційної війни як постійного процесу в світовій політиці, зокрема, ролі ініціаторів та жертв інформаційної агресії. Дослідження зосереджується на теоретичних та практичних аспектах інформаційної війни, її еволюції та сучасних методах ведення, а також особливостях інформаційної агресії проти України.

У першому розділі роботи представлено теоретико-методологічні аспекти інформаційної війни: розглянуто визначення цього поняття, класифікацію інформаційних конфліктів, а також сучасні методи та інструменти інформаційної агресії. Зокрема, було проаналізовано ключові підходи до дослідження інформаційних конфліктів, що дозволяє краще зрозуміти механізми їх впливу.

Другий розділ присвячено історичному контексту та еволюції інформаційної війни. У ньому висвітлено розвиток інформаційної війни від античності до сучасності, зокрема вплив технологічного прогресу, Інтернету та соціальних мереж на інформаційні конфлікти. Було досліджено, як

розвиток технологій призвів до зміни підходів до ведення інформаційних війн, підвищуючи їх ефективність та масштабність.

У третьому розділі основну увагу приділено інформаційній агресії проти України. Розглянуто специфіку та методи ведення інформаційної війни проти українського суспільства, а також її соціально-політичні наслідки. Проаналізовано заходи протидії, здійснювані Україною, та окреслено перспективи розвитку інформаційної безпеки у контексті сучасних викликів.

Результати дослідження показали, що інформаційна війна є значним фактором, який впливає на суспільство, формує громадську думку та використовує маніпулятивні методи для досягнення політичних цілей. Запропоновані рекомендації спрямовані на підвищення ефективності заходів протидії інформаційній агресії та захисту національних інтересів України. Робота підкреслює важливість розвитку інформаційної гігієни та зміцнення інформаційної безпеки у контексті глобалізації інформаційного простору.

ЗМІСТ

Вступ.....	
РОЗДІЛ 1. ТЕОРЕТИКО МЕТОДОЛОГІЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ ВІЙНИ.....	
1.1 Стан наукової розробки дослідження.....	
1.2 Ключові підходи до дослідження інформаційної війни та визначення поняття.....	
1.3 Теоретико- методологічні засади дослідження.....	
1.4 Перманентність інформаційної війни та типологія інформаційних конфліктів: сучасні методи агресії.....	
РОЗДІЛ 2. ІСТОРИЧНИЙ КОНТЕКСТ ТА ЕВОЛЮЦІЯ ІНФОРМАЦІЙНОЇ ВІЙНИ.....	
2.1 Інформаційна війна у минулому.....	
2.2 Історична еволюція та основні характеристики інформаційної війни.....	

2.3	Вплив інформаційної технології на інформаційні конфлікти.....
2.4	Ініціатори та методи інформаційної агресії.....
РОЗДІЛ 3. УКРАЇНА У КОНТЕКСТІ ІНФОРМАЦІЙНОЇ ВІЙНИ.....	
3.1	Інформаційна війна для України як засіб протидії агресії.....
3.2	Методи ведення інформаційної війни проти України та її особливості.....
3.3	Соціально-політичні наслідки інформаційної війни.....
3.4	Заходи протидії інформаційній агресії в Україні та перспективи розвитку.....

Вступ

Актуальність дослідження інформаційної війни стає особливо важливим в умовах сучасних глобальних і регіональних конфліктів, зокрема на прикладі війни Росії проти України. Інформаційна війна — це не лише потужний інструмент впливу на суспільство, але й зброя, здатна змінювати перебіг військових і політичних подій. Сучасні технології та швидкий доступ до інформації створюють умови для ефективної пропаганди, маніпуляцій, формування помилкових уявлень, які можуть дестабілізувати держави та впливати на міжнародні відносини.

Конфлікт між Росією та Україною демонструє не лише використання зброї в традиційному сенсі, але й ведення активної інформаційної кампанії з метою маніпуляції громадською думкою як на національному, так і на міжнародному рівні. Росія постійно використовує пропаганду та дезінформацію, щоб виправдати свої дії та дискредитувати Україну в очах міжнародної спільноти. Це включає в себе поширення фейкових новин, перекручування фактів та створення псевдоісторичних наративів для легітимації своїх дій.

Особливо актуальним це питання стає на фоні розповсюдження соціальних мереж, де інформація поширюється швидко та часто без належної перевірки. Тому тема дослідження інформаційної війни є надзвичайно важливою для розуміння сучасних методів ведення гібридних війн, де інформація стає не менш значущою зброєю, ніж ракети чи танки.

Об'єктом дослідження є явище інформаційної війни, яке стало однією з ключових форм сучасних конфліктів. Воно включає різні методи впливу на громадську свідомість, інформаційне середовище та політичні процеси для досягнення стратегічних цілей. Інформаційна війна є потужним інструментом маніпуляції, що впливає на глобальні відносини, національну безпеку та соціальні структури.

Предметом дослідження є інформаційна війна в Україні, з акцентом на специфіку її ведення у контексті сучасних викликів, методи захисту та їхній вплив на соціальні та політичні процеси в країні.

Дослідження інформаційної війни дозволить глибше зрозуміти, як агресори використовують ці інструменти для підриву національної безпеки, а також визначити ефективні методи протидії. Це надає не лише теоретичне підґрунтя, але й практичні рекомендації для зміцнення інформаційної безпеки держави, а також для розробки стратегій боротьби з пропагандою та дезінформацією.

Керуючись цим, актуальність цієї роботи обумовлена необхідністю поглибленого аналізу нових форм війни, що виходять за межі традиційних військових дій, та розробки ефективних заходів для захисту національної інформаційної сфери від зовнішньої агресії.

Мета даного дослідження полягає в комплексному аналізі трансформації інформаційної війни протягом історії, а також виявленні ролі ініціаторів і жертв у цьому процесі. По-перше, робота досліджує еволюцію методів і підходів, починаючи від античних часів і завершуючи сучасними

тенденціями в інформаційних конфліктах, що надає розуміння, як інформаційна війна адаптувалася до нових технологічних умов. По-друге, метою є детальне дослідження, хто є ініціаторами інформаційних атак і хто стає їхніми жертвами. Це включає аналіз політичних і державних акторів, а також суспільств, що піддаються цим атакам.

Важливим аспектом роботи є дослідження питання України в контексті інформаційної війни. Україна стала центром численних інформаційних атак, особливо після початку збройного конфлікту з Росією у 2014 році. Мета полягає у вивченні українських методів оборони: як держава та суспільство реагують на інформаційну агресію, які інструменти використовуються для протидії та яким чином ці методи впливають на стабільність суспільства. Окремо досліджується, як інформаційні атаки впливають на суспільну думку, емоційний стан населення та політичну ситуацію в Україні, а також які стратегії можна вважати ефективними у протидії дезінформації й маніпуляціям.

Методологічна основа дослідження ґрунтується на міждисциплінарному підході, використовуючи інструменти аналізу з політології, комунікацій, соціології та історії. До основних методів належать аналіз історичних джерел, порівняння різних моделей інформаційних конфліктів, а також вивчення сучасних інформаційних технологій. Особлива увага приділяється дослідженню сучасних методів інформаційної агресії та оборони, зокрема, впливу Інтернету та соціальних мереж.

Наукова новизна полягає в тому, що питання інформаційної війни проти України активно досліджується у зв'язку з поточним конфліктом, проте зосередженої уваги на трансформації методів інформаційного впливу через історичний контекст досі бракує. Існує значна кількість наукових робіт, але вони часто зосереджуються на загальних аспектах без глибокого аналізу сучасних технологій і новітніх форм інформаційної агресії.

Практичне значення цієї роботи полягає в підвищенні усвідомлення інформаційної війни та її впливу на суспільство. Розуміння механізмів маніпуляції інформацією може допомогти людям критично сприймати новини та події, що відбуваються в світі. Крім того, результати дослідження можуть слугувати основою для розробки практичних стратегій протидії інформаційній агресії, що є важливим для організацій і держав. Вивчення цієї теми також може бути інтегровано в навчальні програми, сприяючи підвищенню медіаграмотності населення. Аналіз конкретних випадків інформаційних кампаній дозволить виявити нові тактики агресорів і допоможе у формуванні адекватних відповідей, а також може стати основою для міжнародної співпраці в сфері безпеки та обміну інформацією.

Апробація. Результати досліджень викладено в тезах:

- «Російсько-Українська інформаційна війна: особливості та прояви», Шевченко Н. В. на міжнародній дистанційній науково-практичній конференції «Україна та світ в умовах російської збройної інтервенції(з 2014 р.)» червень 2024 р.

- «Інформаційно-комунікаційна політика ЄС: досвід, проблеми та перспективи» . Всеукраїнський науково-практичний вебінар «Європейський вибір України: історичний аспект, сьогодення та перспективи» травень 2024

- «Вплив дезінформації на відносини України та ЄС: стратегії протидії в епоху інформаційної війни» . Всеукраїнський науково-практичний вебінар «Цілі сталого розвитку України в пан'європейському контексті» вересень 2024р.

- «Міжкультурна комунікація в умовах інформаційної війни: виклики та можливості». Науково-практичний семінар «Міжкультурна комунікація очима молодих науковців», листопад 2024р.

- «ООН у епоху інформаційних війн: виклики для глобального миру та безпеки». Всеукраїнський круглий стіл «ООН

напередодні свого ювілею: діяльність, бездіяльність, перспективи існування» жовтень 2024.

Структура роботи. Робота складається зі вступу, трьох розділів, що мають свої підрозділи, висновків до розділів, загального висновку, списку використаних джерел та додатків. Загальний обсяг роботи сторінок, з них сторінок основного тексту. Для написання роботи використано літературних джерела.

Розділ 1

Частина 1.1

У сучасному світі інформація стала не лише важливим ресурсом, але й ключовим фактором, який суттєво впливає на формування свідомості людей, їхні переконання та поведінку. Вона стала невід'ємною частиною нашого повсякденного життя, проникнувши в усі сфери діяльності людини. Інформація визначає хід міжнародних відносин, впливає на політичні рішення та може стати потужним інструментом впливу або навіть зброєю в руках тих, хто вміло нею користується [Головченко В. І., Гондюл В. П., Зернецька О. В. та ін., 2006].

З розвитком глобалізації та зростанням взаємозалежності між країнами роль інформації в суспільстві значно зросла. В умовах глобальної інтеграції, стрімкого розвитку інформаційних технологій та комунікаційних засобів інформаційна війна перетворилася на одну з найефективніших та найнебезпечніших форм сучасного конфлікту. Сьогодні вона стає невід'ємною складовою геополітичних стратегій держав, корпоративних інтересів та навіть міжособистісних взаємин.

Інформація, завдяки своїй здатності швидко поширюватися та впливати на великі маси людей, стала стратегічним ресурсом, порівняним за значенням з енергетичними чи природними ресурсами. Контроль над інформаційними потоками дозволяє формувати суспільну думку, впливати на економічні процеси та політичні рішення, створювати або руйнувати репутацію, стимулювати або гальмувати соціальні зміни.

Для повного розуміння значення та наслідків інформаційної війни необхідно детально розглянути, що саме означає цей термін, які його складові, методи та інструменти, а також які наслідки вона може мати для суспільства та держави. Інформаційна війна — це не лише набір технологій та методів, але й комплексна система впливу на свідомість та поведінку людей через маніпуляцію інформацією.

Важливо також зрозуміти, як інформаційна війна впливає на міжнародні відносини, політичну стабільність та безпеку держав. В умовах, коли інформаційні технології стають дедалі доступнішими, а інформаційні потоки — дедалі більш неконтрольованими, ризики, пов'язані з інформаційною агресією, значно зростають. Держави та недержавні актори можуть використовувати інформаційну війну для досягнення своїх стратегічних цілей без прямого військового втручання, що робить цей вид конфлікту особливо небезпечним.

Георгій Почепцов, український дослідник інформаційних війн: "Інформаційна війна - це комунікативна технологія по впливу на масову свідомість з короткостроковими і довгостроковими цілями. Цілями такого впливу на масову свідомість є внесення змін у когнітивну структуру з тим, щоб отримати відповідні зміни в поведінковій структурі". [Почепцов Г. Сучасні інформаційні війни. Київ: Києво-Могилянська академія, 2015.]

Мартін Лібікі, американський дослідник: "Інформаційна війна - це використання інформації для досягнення національних цілей". [Libicki M.C.

What Is Information Warfare? Washington, D.C.: National Defense University, 1995.]

Володимир Горбулін, український вчений: "Інформаційна війна - це один з ключових компонентів гібридної війни, який передбачає використання спеціальних інформаційних операцій та технологій для досягнення переваги над противником у інформаційному просторі". [Горбулін В. Світова гібридна війна: український фронт. Київ: НІСД, 2017.]

Девід Аланд, американський експерт з кібербезпеки: "Інформаційна війна - це дії, спрямовані на захист, експлуатацію, пошкодження, руйнування або модифікацію інформації та інформаційних систем противника з метою досягнення значних переваг, цілей або перемоги над противником". [Alberts D.S., Garstka J.J., Stein F.P. Network Centric Warfare: Developing and Leveraging Information Superiority. CCRP Publication Series, 2000.]

Євген Магда, український політолог: "Інформаційна війна - це комплекс заходів інформаційного впливу на масову свідомість для зміни поведінки людей і нав'язування їм цілей, які не відповідають їхнім інтересам, а також захист від такого впливу". [Магда Є. Гібридна війна: вижити і перемогти. Харків: Віват, 2015.]

Пітер Померанцев, британський журналіст та дослідник: "Зброя, яка атакує наше сприйняття реальності, підриваючи саму ідею об'єктивної істини і замінюючи її множинними, суперечливими наративами". [Pomerantsev P. This Is Not Propaganda: Adventures in the War Against Reality. New York: PublicAffairs, 2019.]

Річард Шафранські, полковник ВПС США у відставці: "Інформаційна війна - це діяльність, спрямована проти будь-якої частини системи знань та переконань противника. Незалежно від того, чи ведеться вона проти зовнішнього противника, або проти внутрішніх груп". [Szafranski R. A Theory of Information Warfare: Preparing For 2020. Airpower Journal, Spring 1995.]

Джон Аркілла та **Девід Ронфельдт**, дослідники RAND Corporation: "Інформаційна війна - це конфлікт, в якому інформація є головним ресурсом як для ведення конфлікту, так і для його вирішення". [Arquilla J., Ronfeldt D. In Athena's Camp: Preparing for Conflict in the Information Age. RAND Corporation, 1997.]

Едвард Волц, американський експерт з інформаційних операцій: "Інформаційна війна - це використання інформації як зброї в конфлікті. Вона включає збір, передачу, захист, маніпулювання, спотворення та заперечення інформації". [Waltz E. Information Warfare: Principles and Operations. Artech House Publishers, 1998.]

Григорій Перепелиця, український політолог: "Інформаційна війна - це форма ведення інформаційного протистояння між різними суб'єктами (державами, неурядовими, економічними та іншими структурами), яка передбачає проведення комплексу заходів з нанесення шкоди інформаційній сфері конкуруючої сторони і захисту власної інформаційної безпеки". [Перепелиця Г.М. Генезис конфліктів на посткомуністичному просторі Європи. Київ: Стилос, 2003.]

Дороті Денінг, американська експертка з кібербезпеки: "Інформаційна війна - це сукупність операцій, які порушують або захищають інформацію та інформаційні системи з метою досягнення інформаційної переваги в різних сферах конфлікту". [Denning D.E. Information Warfare and Security. Addison-Wesley, 1998.]

Герберт Лін, американський експерт з кібербезпеки: "Інформаційна війна - це використання інформаційних технологій та інформаційного контенту для досягнення політичних та військових цілей". [Lin H. Cyber Conflict and National Security. Georgetown Journal of International Affairs, 2012.]

Олександр Курбан, український дослідник соціальних комунікацій: "Інформаційна війна - це комплекс інформаційних технологій, методів та засобів, спрямованих на досягнення інформаційної переваги, які застосовуються системно та узгоджено, відповідно до єдиного замислу та плану". [Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі. Київ: ВІКНУ, 2016.]

Інформаційна війна є комплексним явищем, яке включає в себе різноманітні форми та методи впливу на інформаційний простір противника з метою досягнення політичних, економічних або військових переваг. Вона охоплює як технічні аспекти — кібератаки, зломи інформаційних систем, так і психологічні операції, спрямовані на зміну свідомості та поведінки людей.

Ключовими напрямками досліджень інформаційної агресії є вивчення механізмів поширення дезінформації, психологічних аспектів сприйняття інформації, методів виявлення інформаційних атак, впливу інформаційної агресії на політичні процеси, ролі штучного інтелекту в інформаційній агресії, правових аспектів протидії, стратегій медіаграмотності, аналізу наративів та дискурсів, ролі традиційних ЗМІ та впливу інформаційної агресії на національну безпеку [Bradshaw S., Howard P.N., 2018].

Дослідники вивчають, як фальшиві новини та маніпулятивний контент розповсюджуються в соціальних мережах, аналізують алгоритми рекомендацій, вірусне поширення та роль емоційного забарвлення в популяризації неправдивої інформації [Lazer D.M.J. та ін., 2018]. Вивчаються когнітивні упередження та фактори, що впливають на сприйняття і поширення інформації, феномени "ехо-камер" та "інформаційних бульбашок" [Pariser E., 2011].

Теоретико-методологічні засади дослідження інформаційної війни включають аналіз різних теоретичних підходів та методів, які використовуються при вивченні цього складного явища. Теоретичні підходи базуються на системному аналізі, де інформаційна війна розглядається як комплексна система взаємодії різних елементів інформаційного простору [Берталанфі Л., 1969]. Комунікативний підхід фокусується на процесах передачі інформації та моделюванні комунікаційних потоків, вивчаючи медіа як посередника в інформаційній війні [Маклюен М., 2003]. Психолого-психічний підхід досліджує вплив інформаційних операцій на психіку та свідомість людини, зосереджуючись на механізмах маніпуляції та переконання [Лебедь Є. М., 2016]. Кібернетичний підхід звертає увагу на технічні аспекти інформаційної війни, включаючи кібербезпеку та захист інформаційних систем і мереж [Denning D.E., 1999]. Соціально-культурний підхід аналізує роль культурних факторів, цінностей та ідеологій, розглядаючи, як інформація впливає на соціальні структури та норми [Гідденс Е., 1991]. Політологічний підхід розглядає інформаційну війну як інструмент зовнішньої та внутрішньої політики держав, аналізуючи її вплив на міжнародні відносини та геополітичні процеси [Nyе J.S., 2004].

Методологічні засади дослідження базуються на міждисциплінарності, поєднуючи методи з різних наукових дисциплін — соціології, психології, політології, лінгвістики, комп'ютерних наук [Почепцов Г., 2015]. Використовуються кількісні методи для збору та аналізу статистичних даних, таких як частота поширення певних повідомлень, активність користувачів у соціальних мережах, масштаби охоплення аудиторії [Babbie E., 2010]. Якісні методи дозволяють глибоко аналізувати зміст інформаційних матеріалів, виявляти приховані смисли, наративи та дискурси, включаючи контент-аналіз, дискурс-аналіз, семіотичний аналіз [Krippendorff K., 2018]. Кейс-стаді (case study) використовуються для дослідження конкретних випадків інформаційних атак або кампаній з метою глибокого розуміння їх механізмів та наслідків [Yin R.K., 2014]. Мережевий аналіз вивчає структуру та динаміку

мережі поширення інформації, виявляючи ключових вузлів та впливових акторів [Wasserman S., Faust K., 1994]. Експериментальні методи проводяться для вивчення реакції людей на певні інформаційні стимули, дослідження ефективності різних методів впливу [Lewandowsky S. та ін., 2012]. Моделювання та симуляція використовуються для прогнозування розвитку інформаційних конфліктів та оцінки ефективності різних стратегій [Axelrod R., 1997].

Методологічні принципи дослідження включають об'єктивність, що передбачає уникнення особистих упереджень та забезпечення неупередженого підходу до аналізу даних; системність, яка вимагає розглядати інформаційну війну як цілісну систему з взаємопов'язаними елементами; валідацію даних, що полягає у перевірці достовірності та надійності джерел інформації, особливо при роботі з онлайн-контентом та соціальними мережами; та етичність, яка передбачає дотримання етичних норм при проведенні досліджень, зокрема захист приватності учасників та конфіденційності даних [Israel M., Hay I., 2006].

Сучасні технології активно використовуються у дослідженні інформаційної війни. Аналіз великих даних (Big Data) та методи машинного навчання застосовуються для виявлення патернів у поширенні інформації, ідентифікації бот-мереж та координації дезінформаційних кампаній [Lazer D.M.J. та ін., 2018]. Соціальні мережі та онлайн-платформи використовуються для збору та аналізу даних про взаємодію користувачів [Pew Research Center, 2018].

Однак методологія дослідження стикається з низкою проблем та викликів. Доступ до даних може бути обмежений з боку платформ соціальних медіа, що ускладнює збір необхідної інформації. Динамічність інформаційного середовища вимагає постійного оновлення методів та інструментів дослідження. Верифікація інформації стає складнішою через поширення дезінформації та анонімність користувачів. Етичні дилеми

виникають у зв'язку з балансом між необхідністю дослідження та правами на приватність, особливо при аналізі персональних даних [Zimmer M., 2010].

Рекомендації щодо методології дослідження включають поєднання кількісних та якісних методів для отримання повнішої картини явища, використання міждисциплінарного підходу із залученням експертів з різних галузей, постійне оновлення методів та інструментів відповідно до технологічних новацій, а також дотримання етичних стандартів та забезпечення конфіденційності даних.

Інформаційні конфлікти можуть набувати різних масштабів та форм, що залежить від цілей, ресурсів та учасників, які беруть у них участь. Вони можуть бути глобальними, коли охоплюють весь світовий інформаційний простір, регіональними, коли зосереджені на певному географічному регіоні, або локальними, спрямованими на обмежену аудиторію [Головченко В. І. та ін., 2006]. Крім того, інформаційні конфлікти можуть бути міждержавними, коли учасниками є держави або їхні офіційні структури, внутрішньодержавними, що відбуваються всередині однієї країни між різними групами або інституціями, або за участю недержавних акторів, таких як терористичні організації, транснаціональні корпорації, хакерські групи чи навіть окремі особи.

Сучасні методи інформаційної агресії постійно еволюціонують, використовуючи новітні технології та інноваційні підходи для максимізації впливу на цільову аудиторію. Це пов'язано з швидким розвитком інформаційно-комунікаційних технологій, що відкриває нові можливості для поширення інформації та маніпулювання свідомістю людей [Denning D.E., 1998].

Одним із найбільш значущих проявів інформаційної агресії є **кіберконфлікти**. Вони включають атаки на інформаційні системи, мережі та критичну інфраструктуру з метою викрадення конфіденційних даних,

порушення нормальної роботи систем або поширення шкідливого програмного забезпечення. Такі атаки можуть мати серйозні наслідки для національної безпеки, економіки та соціальної стабільності країни [Denning D.E., 1998]. Наприклад, кібератака на енергетичну систему може призвести до відключення електроенергії в масштабах цілого регіону, спричиняючи хаос і паніку серед населення. Кібератаки можуть бути спрямовані також на фінансові установи, транспортні системи або медичні заклади, що порушує життєво важливі послуги. Кіберконфлікти часто є складними та багаторівневими, включаючи використання вірусів, троянських програм, фішингу та інших методів проникнення в системи. Держави та недержавні актори можуть використовувати кіберпростір для проведення шпигунства, саботажу або навіть кібервійни, що підкреслює важливість кібербезпеки та міжнародного співробітництва у цій сфері.

У 2007 році Естонія зазнала масованої кібератаки на державні та фінансові установи, що призвело до тимчасового відключення ключових сервісів [Ottis R., 2008]. У 2015 році кібератака на енергетичну систему України спричинила відключення електроенергії для понад 200 000 людей [Lee R.M. та ін., 2016]. Інший приклад — поширення вірусу Stuxnet у 2010 році, який був спрямований на ядерні об'єкти Ірану, порушуючи роботу центрифуг і затримуючи ядерну програму [Langner R., 2011]. Кібератаки такого масштабу демонструють потенціал для завдання значної шкоди без застосування традиційної військової сили, підкреслюючи важливість кібербезпеки в сучасному світі.

Психологічні операції є ще одним важливим методом інформаційної агресії. Вони спрямовані на вплив на емоційний та психологічний стан населення через поширення страху, невпевненості або ненависті. Це може здійснюватися через розповсюдження панічних чуток, викривлення фактів, створення негативних образів певних груп або інституцій [Лебедь Є. М., 2016]. Метою таких операцій є дестабілізація суспільства, підрив довіри до

уряду або інших важливих інституцій, а також маніпулювання громадською думкою для досягнення власних цілей. Психологічні операції можуть включати використання пропагандистських матеріалів, фальшивих новин, маніпулятивних повідомлень та інших засобів впливу на свідомість людей. Вони можуть бути спрямовані як на широке населення, так і на конкретні групи, використовуючи культурні, релігійні або соціальні особливості для підсилення ефекту. Ефективність психологічних операцій залежить від розуміння психології цільової аудиторії та вмілого використання комунікаційних каналів.

Під час конфлікту на сході України проросійські сили використовували ЗМІ для поширення пропаганди, яка зображала український уряд як фашистський режим, що посилювало напруженість і розділяло суспільство [Szostek J., 2017]. Інший приклад — діяльність терористичної організації ІДІЛ, яка через соціальні мережі поширювала жорстокі відео та пропаганду, спрямовану на залякування населення та вербування нових членів [Winter C., 2015]. Психологічні операції також використовувалися під час Холодної війни, коли обидві сторони поширювали пропаганду для підризу морального духу противника та впливу на громадську думку в інших країнах.

Дезінформаційні кампанії — це координоване поширення неправдивої або викривленої інформації з метою введення в оману або маніпулювання громадською думкою. Вони можуть бути спрямовані на дискредитацію політичних лідерів, вплив на виборчі процеси, підризу міжнародних відносин або створення соціальної напруженості [Lewandowsky S. та ін., 2012]. Прикладом може бути поширення фейкових новин про певну подію, яка насправді не відбулася, але здатна викликати сильний емоційний відгук у суспільстві. Дезінформаційні кампанії часто використовують соціальні мережі та інші швидкі канали комунікації для максимального охоплення аудиторії. Вони можуть бути підтримані фейковими акаунтами, ботами та іншими інструментами для штучного розширення впливу.

Дезінформація може підривати довіру до медіа, створювати розкол у суспільстві та ускладнювати прийняття обґрунтованих рішень.

Соціальні мережі відіграють ключову роль у сучасних інформаційних конфліктах. Вони використовуються як інструмент для таргетованого впливу на конкретні групи населення, поширення вірусного контенту та створення інформаційних бульбашок [Starbird K. та ін., 2019]. Завдяки алгоритмам персоналізації, користувачі отримують інформацію, яка відповідає їхнім уподобанням, що може посилювати когнітивні упередження та обмежувати доступ до альтернативних точок зору. Це створює середовище, де дезінформація та маніпулятивний контент можуть поширюватися швидко і непомітно. Соціальні мережі також дозволяють проводити мікротаргетинг, спрямовуючи специфічні повідомлення на вузькі сегменти аудиторії. Крім того, вони можуть бути використані для координації дій, мобілізації протестів або організації інших масових заходів, що робить їх потужним інструментом як для позитивних, так і для негативних цілей.

Скандал з Cambridge Analytica показав, як дані користувачів Facebook використовувалися для політичної реклами та впливу на вибори в США та Великобританії [Cadwalladr C., Graham-Harrison E., 2018]. У М'янмі соціальні мережі, зокрема Facebook, були використані для поширення мови ненависті проти рохінджа, що сприяло етнічному насильству та гуманітарній кризі [Mozur P., 2018]. Ці приклади демонструють, як соціальні мережі можуть бути використані для маніпулювання громадською думкою та розпалювання конфліктів.

Астротурфінг є технікою, що створює ілюзію масової підтримки певної ідеї або руху через використання фейкових акаунтів, ботів та підставних організацій. Це може вводити в оману громадськість щодо реального рівня підтримки або опозиції до певних питань [Woolley S.,

Howard P.N., 2018]. Наприклад, у соціальних мережах може бути створена велика кількість фейкових профілів, які активно поширюють певні меседжі або коментують публікації, формуючи враження широкого суспільного обговорення та підтримки. Астротурфінг може впливати на громадську думку, створюючи тиск на політиків або інституції, а також підривати легітимність реальних громадських рухів. Виявлення астротурфінгу є складним завданням, оскільки він маскується під справжню активність громадян, що вимагає розробки спеціалізованих методів аналізу та моніторингу.

Під час анексії Криму в 2014 році були виявлені ботоферми, що поширювали проросійські наративи в соціальних мережах, створюючи враження широкої підтримки дій Росії [Fredheim R., 2018]. Інший приклад — фальшиві екологічні групи, створені енергетичними компаніями для протидії законодавству про зміну клімату, які видавали себе за громадські ініціативи [Brulle R.J., 2013]. Астротурфінг може значно впливати на політичні рішення та громадську думку, маскуючи реальні інтереси за фасадом масової підтримки.

Використання технологій **deepfake** стало новим викликом в інформаційній агресії. Ці технології дозволяють створювати фальшиві відео та аудіо, які виглядають як реальні, і можуть бути використані для дискредитації осіб, поширення неправдивої інформації або провокування конфліктів [Chesney R., Citron D., 2019]. Наприклад, може бути створене відео, де політик нібито робить скандальну заяву, що може вплинути на його репутацію та політичну кар'єру. Deepfake технології стають дедалі доступнішими, що підвищує ризик їх використання зловмисниками. Це створює серйозні виклики для медіа, правової системи та суспільства в цілому. Розробка технологій для виявлення deepfake та освітні кампанії щодо критичного сприйняття інформації є важливими кроками для протидії цьому явищу.

Діпфейк-відео з колишнім президентом США Бараком Обамою було створено у 2018 році, де він нібито робить образливі заяви, демонструючи потенціал таких технологій для маніпуляції [Vincent J., 2018]. У 2019 році фальшиве відео зі спікером Палати представників США Ненсі Пелосі, де вона виглядала п'яною, поширилося в соціальних мережах, викликаючи сумніви щодо її компетентності [BBC News, 2019]. Такі випадки підкреслюють ризики deepfake для довіри до інформації та необхідність розробки технологій для їх виявлення.

Крім зазначених методів, важливу роль відіграє **інформаційний тероризм**, який передбачає використання інформаційних технологій та засобів масової інформації для залякування, деморалізації або дестабілізації суспільства з метою досягнення політичних або ідеологічних цілей [Weimann G., 2004]. Терористичні організації активно використовують інтернет та соціальні мережі для поширення своєї пропаганди, вербування нових членів та координації дій. Вони можуть розповсюджувати екстремістські ідеї, відео насильницьких дій або погрози, спрямовані на залякування населення. Інформаційний тероризм ускладнює боротьбу з тероризмом, оскільки інтернет надає можливість діяти анонімно та глобально, перетинаючи національні кордони.

Терористичні організації, такі як Аль-Каїда та ІДІЛ, активно використовують інтернет та соціальні мережі для поширення своєї пропаганди, вербування нових членів та координації дій [Conway M., 2017]. Наприклад, ІДІЛ створювала професійні відео з насильницьким контентом, щоб залякати противників та привабити радикально налаштованих осіб з усього світу. У 2013 році терористи використали Twitter для поширення фейкових повідомлень про вибух у Білому домі, що призвело до короткочасного падіння на фондових ринках [Hern A., 2013]. Інформаційний тероризм може мати значні психологічні та економічні наслідки, поширюючи паніку та невпевненість.

Мережева війна або *netwar* є формою конфлікту, де організації, структури та групи використовують мережеві форми організації та стратегії для проведення інформаційних операцій [Arquilla J., Ronfeldt D., 2001]. Це може включати координацію дій через інтернет, використання розподілених мереж для анонімності та стійкості до протидії. Мережева війна характерна для сучасних конфліктів, де традиційні ієрархічні структури поступаються місцем гнучким та децентралізованим мережам. Це ускладнює виявлення та нейтралізацію таких груп, оскільки вони можуть швидко адаптуватися до змін та діяти автономно. Мережева війна може бути використана як державними, так і недержавними акторами, включаючи хактивістів, терористів та кримінальні угруповання.

діяльність хактивістської групи Anonymous, яка організовує кібератаки на урядові та корпоративні сайти, протестуючи проти цензури та корупції [Olson P., 2012]. Під час Арабської весни в 2011 році протестувальники в Тунісі та Єгипті використовували соціальні мережі та мобільні технології для координації дій та обміну інформацією, що сприяло успішним революціям [Howard P.N., Hussain M.M., 2013]. Мережева війна демонструє, як децентралізовані групи можуть впливати на політичні процеси через ефективне використання технологій.

Також варто згадати про **економічну інформаційну війну**, де інформація використовується для впливу на економічні процеси, фінансові ринки та ділову репутацію компаній. Це може включати поширення неправдивих фінансових звітів, чуток про банкрутство або інші дії, спрямовані на зниження вартості акцій або підірив конкурентоспроможності [Gertz B., 2000]. Такі інформаційні атаки можуть мати серйозні наслідки для економіки, спричиняючи фінансові втрати, втрату робочих місць та зниження інвестиційної привабливості. Економічна інформаційна війна може бути частиною ширшої стратегії, спрямованої на ослаблення країни або компанії

без застосування військової сили. Це підкреслює важливість інформаційної безпеки та прозорості в економічній діяльності.

У 2013 році компанія Muddy Waters опублікувала звіт з критикою китайської компанії NQ Mobile, що призвело до значного падіння акцій останньої, хоча пізніше звинувачення були спростовані [Bloomberg News, 2014]. Інший приклад — поширення фейкових новин про банкрутство компанії Apple, що призвело до тимчасового зниження вартості її акцій [SEC, 2008].

Радіоелектронна боротьба є ще одним методом інформаційної агресії, який передбачає використання електромагнітного спектру для перехоплення, порушення або блокування комунікацій противника. Це може впливати на військові операції, системи управління та зв'язку [Adamy D., 2001]. Радіоелектронна боротьба може включати глушіння радіосигналів, перехоплення секретних повідомлень, впровадження помилкових даних у системи навігації або управління зброєю. Це дозволяє порушувати координацію дій противника, знижувати ефективність його операцій та отримувати стратегічну перевагу. В умовах сучасних військових конфліктів, де технології відіграють ключову роль, радіоелектронна боротьба стає критично важливою складовою.

Сучасні методи інформаційної агресії також включають використання **мобільних додатків, інтернету речей (IoT) та штучного інтелекту** для збору даних про користувачів, моніторингу їхньої поведінки та таргетованого впливу [Howard P.N., 2015]. Зокрема, мобільні додатки можуть збирати дані про місцезнаходження, уподобання та соціальні зв'язки користувачів, що використовується для більш точного таргетування інформаційних повідомлень.

Важливим аспектом є також **маніпуляція пошуковими системами та алгоритмами**, яка дозволяє впливати на видимість певної інформації в

інтернеті. Це може включати SEO-маніпуляції, використання ботів для підвищення рейтингу контенту або навіть прямий вплив на алгоритми рекомендацій [Introna L.D., Nissenbaum H., 2000].

Усі ці методи інформаційної агресії використовуються в комплексі для досягнення максимального ефекту. Вони часто поєднуються та підсилюють один одного, створюючи багатовимірні інформаційні атаки, які важко виявити та протидіяти. Це вимагає від держав, організацій та окремих осіб підвищеної пильності, розвитку навичок критичного мислення та впровадження технологічних рішень для захисту інформаційного простору.

Сучасний інформаційний простір характеризується високою швидкістю поширення інформації та легкістю доступу до неї, що робить суспільство більш вразливим до інформаційних атак. Водночас технології стають дедалі складнішими, а методи маніпуляції — витонченішими. Це створює нові виклики для національної безпеки та вимагає розробки ефективних стратегій протидії інформаційній агресії [Pomerantsev P., 2019].

Однією з ключових особливостей інформаційної війни є її всепроникність. Вона може здійснюватися як у воєнний, так і в мирний час, впливаючи на всі сфери суспільства: політику, економіку, культуру, соціальні відносини. Інформаційна війна може бути прихованою або відкритою, спрямованою на масову аудиторію або на конкретні цільові групи.

Інформаційна війна є невід'ємною та постійною складовою міжнародних відносин, і це пояснюється низкою факторів, які роблять її перманентним явищем. По-перше, боротьба за вплив та контроль над інформаційним простором існує стільки ж, скільки існують міждержавні відносини. У різні історичні епохи держави та інші актори використовували інформацію як інструмент для досягнення своїх стратегічних цілей, впливу на ворогів та зміцнення власних позицій [Почепцов Г., 2015]. Наприклад, ще

в давнину правителі використовували пропаганду та дезінформацію для підвищення своєї легітимності та ослаблення супротивників.

З розвитком технологій можливості для проведення інформаційних операцій значно зросли. Сучасні засоби комунікації дозволяють миттєво передавати інформацію на великі відстані, охоплюючи величезні аудиторії. Це створює умови для постійного використання інформаційних інструментів у міжнародних відносинах, оскільки вони стають ефективним засобом впливу без прямого застосування військової сили [Denning D.E., 1999]. Інтернет, мобільні технології та соціальні мережі дозволяють поширювати повідомлення з неймовірною швидкістю, що робить інформаційні операції більш потужними та впливовими.

Глобалізація та інтеграція світової спільноти сприяють збільшенню значення інформації. Інформаційна взаємозалежність держав робить їх вразливими до зовнішнього впливу, що стимулює їх до постійного моніторингу та захисту свого інформаційного простору [Castells M., 2010]. Економічні, політичні та культурні процеси все більше переплітаються, створюючи середовище, в якому інформаційні атаки можуть мати глобальні наслідки.

Сучасні міжнародні відносини характеризуються високим рівнем конкуренції між державами за політичний, економічний та військовий вплив. У такому контексті інформаційна війна стає інструментом, який дозволяє досягати стратегічних цілей з мінімальними витратами та ризиками [Libicki M.C., 1995]. Інформаційні операції можуть бути прихованими, що ускладнює їх виявлення та відповідь на них, що робить їх привабливими для держав, які прагнуть посилити свій вплив без прямої конфронтації. Наприклад, втручання у виборчі процеси інших країн через кібернетичні атаки та дезінформацію стало реальністю сучасної геополітики.

Постійна присутність інформаційної війни у міжнародних відносинах також пояснюється тим, що інформація є ключовим ресурсом у формуванні громадської думки та легітимації політичних рішень. Держави використовують інформаційні інструменти для впливу на внутрішню та зовнішню аудиторію, формуючи позитивний імідж, виправдовуючи свої дії на міжнародній арені та дискредитуючи опонентів [Горбулін В., 2017]. Медіа-кампанії, культурна дипломатія та освітні програми стали невід'ємними елементами зовнішньої політики багатьох країн.

Інформаційна війна стає перманентною через те, що технологічний прогрес постійно відкриває нові можливості для впливу. Розвиток інтернету, соціальних мереж, мобільних комунікацій та штучного інтелекту створює нові платформи та інструменти для проведення інформаційних операцій [Howard P.N., 2015]. Алгоритми соціальних медіа дозволяють точно таргетувати аудиторію, використовуючи дані про поведінку користувачів для максимізації впливу повідомлень.

Крім того, сучасні конфлікти все частіше набувають гібридного характеру, поєднуючи традиційні військові дії з інформаційними, економічними та кібернетичними операціями. У таких умовах інформаційна війна є постійним елементом стратегії, спрямованої на досягнення переваги над противником на різних рівнях [Murray W., Mansoor P.R., 2012]. Наприклад, під час військових конфліктів інформаційні операції використовуються для підриву морального духу противника, поширення дезінформації та впливу на міжнародну громадську думку.

Важливо також відзначити, що інформаційна війна не обмежується періодами відкритих конфліктів. Навпаки, вона активно ведеться і в мирний час, коли держави прагнуть зміцнити свій вплив, просунути свої цінності та норми, вплинути на політичні процеси в інших країнах [Nye J.S., 2004]. Це робить інформаційну війну постійним явищем, яке не має чітких початку та

кінця. Культурна експансія, інформаційне проникнення та ідеологічний вплив стають інструментами "м'якої сили" у міжнародних відносинах.

Інформаційна війна також стає перманентною через зростання ролі недержавних акторів, таких як транснаціональні корпорації, терористичні організації, хакерські групи та громадські рухи. Вони використовують інформаційні інструменти для досягнення своїх цілей, часто діючи поза межами традиційних державних структур [Arquilla J., Ronfeldt D., 2001]. Соціальні медіа надають їм можливість мобілізувати підтримку, поширювати ідеї та координувати дії на глобальному рівні.

У сучасному світі інформація стала зброєю масового впливу, яка може бути використана для підриву економіки, дестабілізації політичної системи, посилення соціальної напруженості або зміни світогляду населення. Цей факт робить інформаційну війну постійним фактором, з яким держави мають рахуватися та розробляти стратегії захисту та протидії [Pomerantsev P., 2019]. Наприклад, економічні санкції можуть супроводжуватися інформаційними кампаніями, спрямованими на дискредитацію країни в очах міжнародної спільноти.

Нарешті, перманентність інформаційної війни обумовлена тим, що інформаційний простір не має чітких кордонів та регуляторних механізмів, які б обмежували можливості для проведення інформаційних операцій. Міжнародне право ще не виробило ефективних інструментів для регулювання діяльності в інформаційному просторі, що створює вакуум, який може бути використаний для агресивних дій [Schmitt M.N., Vihul L., 2017]. Це ускладнює процес притягнення до відповідальності за кібератаки та дезінформаційні кампанії.

Отже, інформаційна війна є перманентним явищем у міжнародних відносинах через поєднання історичних, технологічних, політичних та соціальних факторів. Вона постійно еволюціонує, адаптуючись до нових

умов та викликів, що робить її невід'ємною складовою сучасного світу. Держави та суспільства повинні бути готовими до цих викликів, розробляючи стратегії захисту та ефективної протидії.

Зважаючи на це, важливим є розвиток комплексних підходів до інформаційної безпеки, що включають технологічні, правові та освітні заходи. Підвищення рівня медіаграмотності населення, розвиток критичного мислення та усвідомлення небезпек дезінформації є ключовими для створення стійкого суспільства [Lewandowsky S. та ін., 2012]. Крім того, міжнародна співпраця в галузі кібербезпеки та боротьби з дезінформацією може стати ефективним засобом протидії глобальним інформаційним загрозам.

Сучасні технології, такі як штучний інтелект та машинне навчання, можуть бути використані як для посилення інформаційної агресії, так і для її виявлення та нейтралізації [Howard P.N., 2015]. Розробка інструментів для автоматичного виявлення фейкових новин, бот-мереж та інших загроз є важливим напрямком наукових досліджень.

Висновок розділ 1

Інформаційна війна стала не лише ключовим елементом сучасних конфліктів, але й перманентним явищем міжнародних відносин. Вона постійно присутня у взаємодії між державами та недержавними акторами, використовуючи інформацію як зброю для впливу на суспільство, політичні процеси та глобальну безпеку. Інформаційна війна включає маніпуляцію інформацією, дезінформацію та пропаганду, спрямовані на зміну громадської думки, підрив довіри до інституцій та досягнення стратегічних цілей без прямого застосування військової сили.

Розвиток сучасних технологій, зокрема інтернету, соціальних мереж і мобільних комунікацій, значно розширив можливості швидкого та масового

поширення інформаційних впливів. Це створює умови для постійного використання інформаційних інструментів у міжнародних відносинах, роблячи інформаційну війну невід'ємною складовою глобальної політики. Важливо усвідомлювати, що інформаційна війна ведеться не лише під час відкритих конфліктів, але й у мирний час, коли держави та інші актори прагнуть зміцнити свій вплив, просунути власні інтереси та вплинути на політичні процеси в інших країнах.

Дослідники підкреслюють необхідність комплексного підходу до вивчення інформаційної агресії, що поєднує аналіз історичних, технологічних, політичних і соціальних факторів. Важливо не лише виявляти дезінформацію та маніпулятивні техніки, але й розробляти ефективні стратегії протидії. Серед них — підвищення медіаграмотності та критичного мислення у населення, вдосконалення законодавчої бази, розвиток технологічних засобів захисту та міжнародна співпраця у сфері інформаційної безпеки. Це допоможе суспільству ефективно протистояти деструктивним інформаційним впливам, зміцнити стійкість перед такими загрозами та зберегти демократичні цінності в умовах перманентної інформаційної війни.

Розділ 2

2.1

Інформаційна війна - це сучасне явище, але її коріння сягає глибокої давнини. Починаючи з доісторичних цивілізацій, інформація використовувалася як потужний інструмент впливу на суспільство та досягнення політичних цілей. Протягом історії людство вдосконалювало методи маніпулювання інформацією, які дозволяють правителям і державам контролювати громадську думку та формувати образ своїх ворогів.

Перші сліди інформаційних маніпуляцій можна простежити ще в античності. У Стародавньому Єгипті фараони використовували монументальні споруди та ієрогліфічні написи для утвердження своєї божественної влади. У Стародавній Греції софісти розвинули мистецтво риторики, яке часто використовувалося для маніпулювання громадською думкою в політичних дебатах. У Римській імперії імператори майстерно використовували монети, статуї та написи для просування свого іміджу та демонстрації військових перемог. Ці матеріали не лише відображали велич імператора, але й допомагали створити певний образ його ворогів та

підкорених народів, а також підтримувати владу та стабільність всередині імперії. [Zanker, P. (1988). *The Power of Images in the Age of Augustus*. University of Michigan Press.]

Одним з перших і найвідоміших прикладів інформаційної війни в античності було використання концепції «демонізації» ворога. Римляни майстерно використовували пропаганду та маніпуляцію інформацією для виправдання своїх військових дій і розширення імперії. Наприклад, під час тривалого конфлікту з Карфагеном, відомого як Пунічні війни, римські історики та оратори часто зображували карфагенян як жорстоких варварів, які практикують людські жертвоприношення, зокрема, приношення в жертву дітей богам Молоху. Ці розповіді були поширені серед населення через літературу, театральні постановки та публічні промови, формуючи негативний образ Карфагена в очах римського суспільства.

Таке спотворене зображення противника слугувало декільком цілям. По-перше, воно підвищувало моральну легітимність війни, представляючи її як боротьбу цивілізації проти варварства і жорстокості. По-друге, воно мобілізувало підтримку серед громадян, стимулюючи патріотичні почуття та готовність до жертв заради захисту Риму. По-третє, це підірвало міжнародну репутацію Карфагена, ускладнюючи йому пошук союзників серед інших держав і народів.

Варто зазначити, що сучасні історичні дослідження ставлять під сумнів багато з цих тверджень про карфагенян. Археологічні знахідки та аналіз джерел свідчать про те, що масштаби та характер практик, приписуваних карфагенянам римлянами, були перебільшені або навіть вигадані з пропагандистською метою. Це підкреслює, наскільки ефективною може бути інформаційна війна у формуванні сприйняття ворога і виправданні політичних та військових дій.

Крім того, римляни використовували й інші методи інформаційної війни, такі як поширення чуток, підлив морального духу противника та створення внутрішніх конфліктів у суспільстві Карфагена. Наприклад, вони могли підтримувати опозиційні групи всередині Карфагена або фінансувати повстання в підконтрольних йому територіях, що відволікало ресурси та увагу карфагенян від основного конфлікту з Римом.

Цей історичний приклад демонструє, що навіть у давні часи інформація та її контроль були потужним інструментом у міжнародних відносинах і військових конфліктах. Римляни розуміли важливість формування громадської думки та використовували інформаційну стратегію для досягнення своїх цілей. Це не лише сприяло їхнім військовим перемогам, але й заклало основи для майбутніх підходів до інформаційної війни.

Ця тактика розвинулася в Середньовіччі, коли релігійні та політичні діячі використовували інформацію, щоб спровокувати конфлікт і підірвати авторитет своїх опонентів. Церква відіграла ключову роль у формуванні громадської думки через проповіді, релігійне мистецтво та літературу. **Хрестові походи супроводжувалися масштабною пропагандистською кампанією**, яка зображала мусульман як невірних, яких потрібно навернути або знищити. Папа Урбан II у 1095 році виголосив полум'яну промову на Клермонському соборі, закликаючи християнську Європу об'єднатися проти "спільного ворога" [Keen, S., 1986]. Ця промова була навмисно спрямована на виклик емоційного відгуку, підсилюючи релігійний запал та обіцяючи відпущення гріхів тим, хто вирушить у похід. Проповідники мандрували містами та селами, поширюючи легенди про жорстокість мусульман та необхідність звільнення Святої Землі.

У той же час, **візантійські імператори використовували складну систему дипломатії та пропаганди** для маніпулювання сусідніми державами та збереження своєї влади. Вони розсилали посланців з перекрученими повідомленнями, намагаючись посіяти розбрат між своїми

ворогами. Наприклад, імператор Олексій I Комнін звернувся до папи та західних правителів з проханням про військову допомогу проти сельджуків, одночасно перебільшуючи загрозу, щоб отримати більше підтримки [Kaldellis A., 2017]. Візантія також активно використовувала **шпигунство та контррозвідку**, збираючи інформацію про плани та сили потенційних противників. Через контроль над торгівлею та дипломатичними зв'язками вони поширювали чутки та дезінформацію, щоб послабити коаліції проти себе.

Релігійне мистецтво та література також служили засобами інформаційної війни. Ікони, фрески та реліквії використовувалися для підсилення релігійних почуттів та легітимації влади. Церковні хроністи описували події з точки зору, вигідної для їхніх покровителів, іноді замовчуючи або викривляючи факти. **Єретичні рухи**, такі як катари та вальденси, були піддані репресіям не лише військовими засобами, але й через інформаційну кампанію, яка зображала їх як небезпечних відступників, загрозу для суспільства. Інквізиція активно використовувала допити та тортури для отримання "зізнань", які потім публічно оголошувалися як докази провини.

Університети та наукові центри, які виникли в пізньому Середньовіччі, стали аренами боротьби за контроль над знаннями. Церква намагалася контролювати навчальні програми та обмежувати доступ до певних філософських та наукових творів, які вважалися небезпечними для доктрини. Наприклад, твори Аристотеля були спочатку заборонені, а пізніше дозволені з обмеженнями та коментарями, що відповідали церковному вченню.

Цей період характеризувався інтенсивним інтелектуальним обміном та зростанням інтересу до раціонального пізнання світу. Заснування університетів у містах як Болонья, Париж, Оксфорд і Кембридж створило нові можливості для вивчення права, медицини, теології та мистецтв. Однак Церква прагнула зберегти монополію на інтерпретацію

істини та забезпечити, щоб освіта відповідала релігійним догмам. **Викладання філософії Аристотеля, яка була відома через арабські переклади та коментарі, викликало особливе занепокоєння, оскільки його ідеї про природу, космологію та метафізику могли суперечити біблійному вченню [Dod, V.G., 1982].**

У 1210 році Синод у Парижі заборонив викладання природничих творів Аристотеля, таких як "Фізика" та "Метафізика", без офіційного схвалення. Пізніше, у 1231 році, папа Григорій IX підтвердив цю заборону, але дозволив продовжувати дослідження після внесення необхідних корективів. Це призвело до появи "латинських Аверроїстів", групи вчених, які намагалися поєднати аристотелівську філософію з християнським вченням, що викликало подальші конфлікти з Церквою [Gilson, E., 1955].

Тиск Церкви на університети іноді приводив до переслідувань окремих вчених. Наприклад, англійський філософ Роджер Бекон, відомий своїми експериментальними підходами в науці, був ув'язнений за обвинуваченнями у єресі та чаклунстві [Hackett, J., 1997]. Його роботи з оптики, хімії та мовознавства були далеко попереду свого часу, але викликали підозри через незвичність методів і висновків.

Попри обмеження, університети стали центрами інтелектуальної свободи та критичного мислення. Студенти та викладачі організовували диспути, де обговорювалися спірні питання філософії та теології. Це сприяло розвитку схоластики, методу навчання, який поєднував логіку з теологічним аналізом. Відомі вчені, такі як Фома Аквінський, намагалися інтегрувати аристотелівську філософію з християнською доктриною, що врешті-решт призвело до часткового прийняття цих ідей Церквою [Aquinas, T., 1265–1274].

Зіткнення між традицією та новаторством в університетах пізнього Середньовіччя відображало ширші суспільні зміни. Зростання міст,

розвиток торгівлі та поява нових соціальних класів створили потребу в освіті та знаннях, які виходили за межі церковної доктрини. **Переклади арабських та грецьких наукових праць**, привезені під час хрестових походів та торгових зв'язків, збагачували європейську думку та стимулювали науковий прогрес [Burnett, С., 2001].

Церква, усвідомлюючи неможливість повного контролю над інтелектуальним життям, почала шукати компроміси. Було створено цензурні комісії, які переглядали та схвалювали твори перед їх публікацією. **Інквізиція стала інструментом не лише релігійного, але й інтелектуального контролю**, хоча її діяльність часто зустрічала опір з боку університетської спільноти.

Ця боротьба за знання заклала основи для майбутніх епох Відродження та Просвітництва, коли критичне мислення та науковий метод стали головними цінностями європейського суспільства. **Середньовічні університети перетворилися на осередки інновацій**, сприяючи розвитку філософії, науки та мистецтва. **Конфлікти між Церквою та наукою продовжувалися**, але поступово баланс зміщувався в бік свободи досліджень і вираження думок. Контроль над знаннями ставав все менш ефективним, і нові ідеї почали проникати в суспільство, змінюючи його назавжди.

Розвиток книгодрукування в кінці Середньовіччя почав змінювати ландшафт інформаційної війни, оскільки стало легше поширювати ідеї серед широких мас. Це призвело до Реформації, де інформаційна війна між католиками та протестантами досягла нового рівня. Мартін Лютер використовував друковані памфлети та переклад Біблії на німецьку мову, щоб донести свої ідеї до народу, що підірвало авторитет Римської церкви.

Таким чином, у Середньовіччі інформаційна війна набувала нових форм та масштабів, впливаючи на політичні рішення, суспільні настрої та хід

історії. Релігійні та політичні лідери розуміли силу інформації та активно використовували її для досягнення своїх цілей. **Це заклало основи для сучасних методів інформаційної агресії**, показуючи, що контроль над інформацією є ключовим фактором у боротьбі за владу та вплив. Середньовічний досвід демонструє, що маніпуляція свідомістю та використання пропаганди є давніми практиками, які продовжують розвиватися разом із суспільством.

З розвитком друкарського верстата і появою перших газет у 15 столітті інформаційна війна набула нових форм. Публікації стали основним засобом поширення та обробки політичної ідеології. Реформація Мартіна Лютера була одним з перших рухів, що ефективно використовував друковану пропаганду для поширення своїх ідей. Памфлети та листівки відігравали ключову роль у розпалюванні релігійних конфліктів в Європі. У той же час, монархи використовували друковані матеріали для легітимізації своєї влади та формування національної ідентичності. [Eisenstein, E. L. (1979). *The Printing Press as an Agent of Change*. Cambridge University Press.]

У 19 столітті розвиток масової преси та телеграфу значно прискорив поширення інформації. Газети стали потужним інструментом формування громадської думки та політичної пропаганди. Наприклад, "жовта преса" в США відіграла значну роль у розпалюванні іспано-американської війни 1898 року. У Європі національні рухи активно використовували пресу для поширення своїх ідей та мобілізації підтримки.

Особливого значення інформаційна війна набула у 20 столітті з розвитком засобів масової інформації. Перша світова війна стала першим конфліктом, де пропаганда використовувалася систематично всіма сторонами. Створювалися спеціальні урядові органи для координації пропагандистських зусиль.

Під час Другої світової війни пропаганда досягла нового рівня складності та ефективності. Нацистська Німеччина під керівництвом міністра пропаганди Йозефа Геббельса створила потужну машину для маніпулювання громадською думкою, використовуючи радіо, кіно та друковані ЗМІ. Союзники також активно використовували пропаганду, включаючи психологічні операції проти ворожих військ. [Welch, D. (2002). *The Third Reich: Politics and Propaganda*. Routledge.]

Холодна війна між СРСР і США та їхніми союзниками у 1946-1991 роках є класичним прикладом інформаційної війни, яка не переросла у збройний конфлікт. Обидві сторони використовували широкий спектр методів інформаційного впливу, включаючи радіомовлення (наприклад, "Голос Америки" та "Радіо Свобода"), кінопропаганду, культурну дипломатію та таємні операції. Радянські операції з дезінформації, такі як операція "Інфекція" (поширення чуток про походження СНІДу), вплинули на формування сучасних підходів до інформаційної війни. [Bittman, L. (1985). *The KGB and Soviet Disinformation: An Insider's View*. Pergamon-Brassey's.]

У 1992 році поняття «інформаційна війна» вперше офіційно згадується в директиві Пентагону, що відображає зростаюче усвідомлення важливості інформації у військових та геополітичних стратегіях. Наприкінці 20-го - на початку 21-го століть інформаційна війна набула нових форм з появою Інтернету та соціальних мереж. Кібератаки, фейкові новини, маніпуляції в соціальних мережах стали новими інструментами інформаційного протиборства. Події, такі як втручання у вибори в США 2016 року та інформаційні кампанії навколо пандемії COVID-19, демонструють масштаб і вплив сучасної інформаційної війни. [Libicki, M. C. (1995). *What Is Information Warfare?* National Defense University.]

За даними ВООЗ, під час пандемії COVID-19 відбувся сплеск дезінформації, що отримав назву "інфодемія". Дослідження виявили, що 70% людей зіткнулися з фальшивими новинами про COVID-19, а 20% населення

світу почали сумніватися в ефективності вакцин через поширення дезінформації в соціальних мережах. [WHO Report on COVID-19 Infodemic, 2020].

Американський соціолог Елвін Тоффлер у своїй роботі "Третя хвиля" поділяє суспільний розвиток на «три хвилі», де в постіндустріальному суспільстві влада належить тим, хто володіє знаннями, інтелектом і, найголовніше, інформацією:

- Хвиля 1: охоплює період аграрного суспільства, який тривав від початку землеробства приблизно 8000 років до н.е. до кінця XVIII століття. У цей час основою економіки було сільське господарство, і більшість населення займалася землеробством та тваринництвом. Головним ресурсом була земля, а влада належала тим, хто контролював землю та природні ресурси. Влада була сконцентрована в руках землевласників, монархів та аристократії. Суспільство було ієрархічним, з чітким розподілом на стани та класи. Технологічний прогрес був повільним, зосередженим на вдосконаленні сільськогосподарських знарядь та методів. Інформація передавалася повільно, через особисте спілкування, письмові повідомлення та гінців. У цьому суспільстві війни велися переважно за території та ресурси, оскільки контроль над землею означав контроль над виробництвом їжі та, відповідно, владу.

- Хвиля 2: почалася з промислової революції в кінці XVIII століття і тривала до середини XX століття. Перехід до індустріального суспільства був спричинений розвитком машинного виробництва, використанням нових джерел енергії та масовим виробництвом товарів. Основним показником сили та впливу стало накопичення капіталу та володіння засобами виробництва. Стандартизація та конвеєрне виробництво дозволили виробляти товари у великих кількостях. Більшість населення переселилася до міст, де знаходилися

заводи та фабрики, що призвело до урбанізації. Технології розвивалися стрімко, особливо в галузях механіки, хімії, транспорту та зв'язку, таких як телеграф і телефон. Соціальна структура змінилася з появою робітничого класу, боротьби за права працівників та зміни соціальної ієрархії. У цей період війни велися за ринки збуту, колонії та ресурси для промисловості, а військова міць базувалася на індустріальному потенціалі держави.

- Хвиля 3: почалася в другій половині ХХ століття і триває до сьогодні. Це епоха інформації та знань, де головним ресурсом стає інформація, а не матеріальні активи. Основним джерелом влади та багатства стають знання, інформація та інтелектуальний капітал. Відбувається децентралізація виробництва, перехід від масового виробництва до гнучких, індивідуалізованих підходів. Розвиток комп'ютерів, інтернету та телекомунікацій змінює спосіб життя та роботи людей. Посилюються зв'язки між країнами, обмін інформацією та культурами в реальному часі, що веде до глобалізації. Зростає роль освіти, з'являються нові професії, пов'язані з інформаційними технологіями, а багато аспектів життя переносяться в цифровий простір.

Це теоретичне осмислення допомагає зрозуміти, чому інформаційна війна стала такою важливою в сучасному світі. [Джерело: Toffler, A. (1980). *The Third Wave*. Bantam Books.]

У третій хвилі війна набуває нових форм та характеристик. Інформація використовується як зброя для впливу на свідомість людей, маніпулювання громадською думкою та підризу політичної стабільності. З'являються кібернетичні війни, які включають атаки на інформаційні системи, мережі та інфраструктуру з метою порушення роботи держави чи компаній. Прогрес в освоєнні космосу дозволяє використовувати космічні технології для комунікацій, спостереження та навігації, що має військове та стратегічне

значення. Комп'ютеризація панування виражається у використанні комп'ютерних систем та штучного інтелекту для контролю, управління та прогнозування.

У постіндустріальному суспільстві інформація стає найціннішим ресурсом. Ті, хто володіє інформацією та вміє її використовувати, отримують значну перевагу в економічній, політичній та соціальній сферах. Сучасне суспільство критично залежить від інформаційних систем у всіх сферах життя — від фінансів до охорони здоров'я. Інформаційні системи можуть бути ціллю кібератак, що призводить до серйозних наслідків для національної безпеки. Завдяки інтернету та соціальним мережам інформація поширюється миттєво, що дозволяє впливати на великі аудиторії в реальному часі. Інформація може бути використана для впливу на вибори, політичні рішення, створення соціальної напруженості. Не лише держави, але й терористичні організації, хакери та корпорації можуть вести інформаційну війну.

У третій хвилі війна зміщується від фізичних бойових дій до інформаційних та кібернетичних операцій. Це включає кібервійни — атаки на комп'ютерні системи, злам баз даних, поширення вірусів. Поширення дезінформації, пропаганди, маніпуляція новинами та соціальними мережами стають частиною інформаційних операцій. Психологічні операції впливають на емоції та поведінку людей через цілеспрямовану інформацію. Економічна війна використовує інформацію для впливу на фінансові ринки та здійснення економічного шантажу. Використання передових технологій, штучного інтелекту та автоматизації забезпечує технологічну перевагу.

Історія надає численні приклади війн з дуже різними засобами, методами, цілями і темами. Інформаційна війна також багато в чому

відрізняється від інших форм війни. Тому, на нашу думку, варто замислитися над відмінностями між інформаційною війною та іншими формами війни.

Кожен тип війни націлений на певний тип території. Якщо це звичайна війна (збройний конфлікт), то основною ціллю є фізична сфера. Якщо це психологічна війна, то головною ціллю є когнітивна сфера. Якщо це інформаційна війна, то головною ціллю є інформаційна сфера. Різниця між цими типами війни полягає в часі. Традиційна мета війни, фізична сфера, вимагає негайної реакції. Інформаційна війна вимагає щоденного планування дій. Психологічна війна вимагає планування на десятиліття.

Основна відмінність психологічної війни від інформаційної полягає в тому, що психологічна війна- це насамперед сукупність засобів і методів, спрямованих на вплив на людей та їхні установки з метою зміни їхніх поглядів, думок, ціннісних орієнтацій, стереотипів, норм, усталених стереотипів, масових настроїв і загальної суспільної свідомості. Інформаційний вплив охоплює не лише суспільну свідомість, але й імідж держави, комп'ютерні системи, системи прийняття рішень, системи розподілу та використання інформаційних ресурсів.

Різниця між збройним конфліктом та інформаційною війною полягає не лише в об'єкті нападу, методах і засобах, але й у ймовірності поразки. На відміну від збройного конфлікту, поразка в інформаційній війні майже неможлива.

Хоча в політології з цього приводу ведеться багато дискусій, за логікою речей, якщо і звичайні ,і інформаційні конфлікти вважати війнами, то поразка в будь-якому конфлікті має бути на боці тієї чи іншої сторони. Єдина відмінність між інформаційною та звичайною війною – це тип зброї, що використовується.

Якщо брати до уваги звичайну війну, то ознаками поразки в таких конфліктах є такі наслідки: скорочення військ, втрата частини території,

політична залежність від переможця, захоплення технологічно складного обладнання, загибель або переміщення частини населення, руйнування промисловості та виплата контрибуції.

В інформаційних війнах можна спостерігати такі ознаки поразки:

- Пошкодження інформаційної системи, зміна або втрата її елементів та підструктурних одиниць. Така деформація або спрощення системи робить її безпечною та вразливою для противника.
- Система виконує завдання, що становлять інтерес для переможця. Система обробляє лише дані, отримані від переможця. Переможена система переймає алгоритм роботи системи переможця. Система безпосередньо засвоюється своїми структурними одиницями та елементами.

Як бачимо, для сторони, що програла, часто не має значення, чи вона програла традиційну війну, чи інформаційну. Різниця між цими двома типами війни полягає в результаті. В інформаційних війнах немає чіткого кінця. Якщо ми говоримо про традиційну війну, то кульмінацією буде підписання мирного договору. Сторона-переможець відмовляється від контролю над інформаційними системами сторони, що програла, ні у фінансовому плані, ні з точки зору безпеки.

У сучасному світі інформаційна війна стала невід'ємною частиною міжнародних відносин, особливо під час конфліктів. Інформаційна війна є потужним інструментом маніпуляції, здатним змінювати не лише сприйняття реальності, а й саму реальність. В умовах глобалізації та стрімкого розвитку цифрових технологій інформаційна війна стала безперервним процесом, який охоплює всі сфери суспільного життя.

Інформаційна війна є надзвичайно складним і багатогранним явищем, що охоплює широкий спектр методів і тактик, спрямованих на вплив на

психологію, поведінку та процеси прийняття рішень різних груп населення. Розвиток цифрових технологій та глобалізація зробили інформаційну війну невід'ємною частиною сучасних конфліктів, що впливає не лише на військові операції, але й на політичні, економічні та соціальні процеси. З кожним етапом розвитку технологій та інформаційного простору тактика інформаційної війни постійно еволюціонувала, пристосовуючись до нових умов і викликів. Сьогодні це вже не просто пропаганда в традиційному розумінні, а складна комбінація інформаційних, психологічних і технологічних впливів, які використовують держави, недержавні актори та навіть приватні компанії для досягнення своїх цілей. [Почепцов Г., *Сучасні інформаційні війни*, 2015]

Перші форми інформаційної війни існували ще в античні часи, коли правителі використовували пропаганду для формування суспільної думки та підтримки серед населення. Проте справжнє розгортання інформаційної війни розпочалося в Новий час, коли технологічні інновації, зокрема друкарський верстат, дозволили значно прискорити поширення інформації. З появою друкарської преси в Європі в XVI столітті, уряди й церковні інституції почали використовувати друковані матеріали як інструмент політичної пропаганди. Це стало початком масового впливу на громадську свідомість через розповсюдження памфлетів, листівок і газет, що містили відповідні наративи та цінності. Одним із яскравих прикладів використання інформації як зброї була Реформація в Європі, коли Мартін Лютер і його послідовники активно використовували друковані видання для поширення своїх ідей і критики католицької церкви. Такі події показали, що інформаційна війна може впливати не лише на політичні процеси, але й на релігійні та соціальні рухи. [Schiller D., *The New Economy of Information*, 2001]

З розвитком друкованих медіа, засобів масової комунікації та поширенням газет у XVIII-XIX століттях, уряди почали усвідомлювати

потенціал маніпуляції інформацією для досягнення політичних і економічних цілей. Більше того, цей період став початком систематичного використання дезінформації як інструменту зовнішньої політики. Французька революція, Наполеонівські війни та зростаючий націоналізм у Європі створили сприятливе середовище для поширення націоналістичних ідей через контрольовані державою друковані ЗМІ. Одним із прикладів є Наполеон Бонапарт, який активно використовував газети для створення іміджу непереможного полководця, розширюючи свій вплив через інформаційну маніпуляцію та пропаганду як всередині Франції, так і за її межами. Його успішне використання контролю над інформаційними потоками дозволяло створювати переможний наратив навіть тоді, коли військові кампанії були невдачливими. Це стало основою для сучасного розуміння інформаційної війни як частини загальної стратегії управління суспільною думкою та впливу на міжнародну політику. [Tulard J., *Napoléon*, 1987]

У ХХ столітті, особливо під час світових воєн, інформаційна війна стала невід'ємною частиною військових кампаній. Важливість пропаганди та дезінформації в управлінні масовою свідомістю та мобілізації ресурсів вийшла на новий рівень із розвитком засобів масової комунікації. Радіо, кіно та плакати перетворилися на потужні інструменти впливу на суспільну думку. Нацистська Німеччина під керівництвом Йозефа Геббельса створила одну з найпотужніших пропагандистських машин в історії. Ця система не лише підтримувала бойовий дух, але й використовувалася для виправдання масових злочинів і геноциду. Контроль над інформаційними потоками дозволяв створювати викривлене уявлення про реальність, що стало характерною рисою тоталітарних режимів ХХ століття. [Herf J., *The Jewish Enemy: Nazi Propaganda during World War II and the Holocaust*, 2006]

Однак коріння такого масштабного використання інформаційної війни сягає Першої світової війни, яка стала одним із перших великих прикладів її впливу на світову політику. Обидві сторони конфлікту активно

застосовували пропаганду для мобілізації населення, дискредитації ворога та підняття морального духу. Велика Британія, наприклад, створила Міністерство інформації для контролю над медіа та поширення пропаганди як всередині країни, так і за її межами. Водночас німецька пропаганда використовувала більш агресивні та маніпулятивні методи. Наприклад, під час битви при Вердені 1916 року німецька преса стверджувала, що французькі військові надають своїм солдатам наркотики, щоб ті могли довше витримувати жахи війни. Це звинувачення не лише дискредитувало французьку армію, але й мало на меті деморалізувати французьке суспільство.

Іншим шокуючим прикладом німецької дезінформації стало звинувачення британських військових у використанні трупів солдатів для виготовлення мила. Це твердження, яке пізніше отримало назву "німецьке мило", мало надзвичайно потужний вплив на світову громадську думку. Німецька пропаганда намагалася представити Британію як варварську державу, що не поважає навіть власних солдатів. Хоча ці звинувачення були вигаданими, вони викликали обурення в міжнародних колах і ще більше загострили ситуацію між воюючими сторонами. Союзники протидіяли цьому шляхом швидкого поширення контрнарративів і залученням нейтральних країн, таких як Нідерланди та Швейцарія, до поширення правдивої інформації. Британська контрпропаганда також акцентувала увагу на воєнних злочинах Німеччини, зокрема, на жорстокості, що чинилися в окупованій Бельгії, де німецькі війська були звинувачені у масових вбивствах і знищенні цивільного населення. Були поширені свідчення очевидців і фотоматеріали, які додавали ваги цим звинуваченням. Такі стратегії заклали фундамент для більш складних форм інформаційної війни, які розвинулися під час Другої світової війни та в подальші десятиліття. [Mock J., Larson J., *The Great War and the British People*, 1976]

З розвитком масових комунікаційних технологій, особливо після Другої світової війни, інформаційна війна стала важливим компонентом протистояння між двома наддержавами – США та СРСР у період Холодної війни. Це протистояння включало не тільки змагання у військовій та економічній сферах, але й інтенсивні інформаційні кампанії з метою ідеологічного впливу на різні частини світу. Радянський Союз активно використовував дезінформацію та інформаційні операції для створення фальшивих новин і документів, що стали основою багатьох операцій, спрямованих на підрив західної демократії. Однією з таких операцій була широко відома кампанія з поширення фейкових новин про те, що вірус СНІД був створений урядом США як біологічна зброя. Ця кампанія, що почалася в 1980-х роках, стала одним із найбільш успішних прикладів радянської дезінформації, впливаючи на глобальну громадську думку та підбиваючи довіру до американських наукових і медичних установ. [Andrew C., Mitrokhin V., *The KGB and the World*, 2005]

Інший яскравий приклад інформаційної війни - операція "Інфекція", проведена КДБ у 1980-х роках. Метою цієї операції було поширення чуток про те, що США розробляють етнічну зброю, здатну вибірково вражати певні расові групи. Ця дезінформація була спрямована на підрив відносин між США та країнами третього світу, особливо в Африці. Операція мала значний успіх, викликавши хвилю антиамериканських настроїв у багатьох країнах. [Boghardt T., *Operation INFEKTION: Soviet Bloc Intelligence and Its AIDS Disinformation Campaign*, 2009]

У 1960-х роках США проводили операцію "Мокінгберд", спрямовану на маніпулювання ЗМІ для просування проамериканських наративів як всередині країни, так і за кордоном. ЦРУ активно співпрацювало з журналістами, видавцями та власниками медіа для формування громадської думки та протидії радянській пропаганді. Ця операція демонструє, як

демократичні країни також могли вдаватися до методів інформаційної війни. [Bernstein C., The CIA and the Media, Rolling Stone, 1977]

Психологічні операції є ще одним важливим елементом інформаційної війни і мають на меті деморалізувати, створити відчуття страху і ненависті, а також мотивувати людей до дії або бездіяльності. Такі операції можуть бути спрямовані як на військових, так і на цивільне населення. Під час війни у В'єтнамі США використовували PSYOPS, скидаючи листівки з деморалізуючими повідомленнями і транслюючи радіопрограми, спрямовані на деморалізацію північно-в'єтнамських солдатів. У сучасному контексті, під час війни між Росією та Україною, російські ЗМІ активно використовували психологічні операції для створення нестабільності та страху в українському суспільстві.

Під час В'єтнамської війни обидві сторони активно використовували інформаційну війну. Північний В'єтнам та В'єтконг проводили психологічні операції, спрямовані на деморалізацію американських військ. Вони поширювали листівки та транслювали радіопередачі, які закликали солдатів здаватися або дезертирувати. США, у свою чергу, проводили операцію "Чорний чоловік", розповсюджуючи чутки про надприродні істоти, які полюють на в'єтнамських солдатів, щоб посіяти страх та паніку. [Landers J., The Weekly War: Newsmagazines and Vietnam, 2004]

У 1980-х роках США запустили програму "Активні заходи", спрямовану на протидію радянській дезінформації. Ця програма включала створення міжвідомчої робочої групи для виявлення та спростування радянської пропаганди. Одним з найбільших успіхів цієї програми було викриття операції КДБ "Панама-3", яка мала на меті дискредитувати США напередодні передачі Панамського каналу. Ця програма демонструє, як інформаційна війна може включати не лише наступальні, але й оборонні стратегії. [Schoen F., Lamb C., Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference, 2012]

«Активні заходи» Томаса Ріда – це всеохоплююча історія дезінформації та операцій впливу протягом останніх 100 років. Рід, який викладає в Школі перспективних міжнародних досліджень Університету Джонса Гопкінса, починає свою розповідь з «Треста», неймовірної операції ЧК на початку 1920-х років, спрямованої на знищення емігрантської царської опозиції. Потім він слідкує за радянськими та російськими операціями дезінформації протягом чотирьох основних етапів: ранніми та хаотичними операціями впливу 1920-х і 30-х років; професіоналізованими операціями першої половини Холодної війни; масштабними бюрократичними активними заходами 1970-х і 80-х років; а потім, після затишшя в 1990-х роках, переходом до операцій, заснованих на Інтернеті, в наш час. З огляду на домінуючу роль Радянського Союзу у створенні цієї форми політичної війни, історія Ріда орієнтована на Москву, хоча він додає чимало інформації про маловідомі операції США в Берліні 1950-х років. Однак, цікаво, що Рід мало говорить про Конгрес культурної свободи та інші операції ЦРУ на підтримку західних антикомуністичних інтелектуалів.

Рід підкреслює, що найуспішніші інформаційні операції Радянського Союзу не покладалися виключно на брехню або підробки. Натомість вони зазвичай будувалися на основі правди, яка надавала достовірності незначній кількості додаткової брехні. Найкращі частини книги – це ті, де Рід описує окремі операції, щоб показати, як цей метод працював на практиці. В одному помітному випадку КДБ злив документи, викрадені Робертом Лі Джонсоном, який шпигував для росіян з початку 1960-х років, коли він був кур'єром армії США в Європі, доки його не заарештували в 1964 році. Пізніше в цьому десятилітті КДБ злив лівим журналістам копії документів, наданих Джонсоном, про плани США щодо використання ядерної зброї в Європі; радянська влада додала лише одну незначну зміну від себе – абзац, який «дозволяє» місцевим командирам використовувати невеликі ядерні заряди в дружніх і нейтральних країнах. Уряд США стверджував, що Москва розповсюджує підробки, але, побоюючись порушити власні правила

класифікації, не вказував, яка частина пакета була підробленою, залишаючи поле дій для радянської влади.

Документи циркулювали роками, надаючи КДБ те, що Рід називає «золотою копальною дезінформацією», яка грала на антиамериканських і антиядерних настроях, щоб сіяти розбрат на Заході. Операція також була типовою в тому, як вона використовувала журналістів, які, хоча й не були агентами КДБ або навіть не симпатизували Москві, були настільки антиамериканськими, що не ставили занадто багато питань про те, що потрапляло в їхні руки. Навіть якщо документи містили підробки, писав один журнал, вони були «достатньо близькими до правди, щоб їх прийняли» – «правдоподібність» ще до свого часу. Радянська влада продовжувала вдосконалювати мистецтво підробок і використання довірливих журналістів, щоб використовувати упередження, підозри та розломи, що вже існували в політиці та культурі Заходу.

Розповідь Ріда про те, як у 1980-х роках КДБ поширював твердження, що уряд США створив вірус СНІДу, є особливо показовою. Він зазначає, що звинувачення в причетності уряду вперше виникли в 1983 році серед активістів гей-спільноти США, які були дуже підозрілими до політичної системи, яка, на їхню думку, ставилася до них як до вигнанців. КДБ, прагнучи відвернути увагу світу від повідомлень про використання радянської хімічної зброї в Афганістані, побачив можливість і швидко розмістив цю історію в індійській газеті, відправивши анонімний лист від «відомого американського вченого», який розмістив історію про СНІД у контексті історії неетичних медичних експериментів уряду в 1960-х і 1970-х роках зробивши СНІД черговим таким епізодом.

Знадобилося кілька років, щоб це твердження потрапило в основні західні та американські ЗМІ, але до 1987 року «невпинне повторення» перенесло його з Індії до активістів на маргінесі в Сполучених Штатах і, нарешті, до «багатьох мільйонів американських домогосподарств у прайм-

тайм новин на великому телеканалі». Крім гей-спільноти, Рід описує, як ця історія особливо резонувала серед афроамериканців, у яких було довге пам'ять про те, як вони ставали мимовільними об'єктами медичних експериментів. Загалом він приходить до висновку, що історія про СНІД, ймовірно, була найуспішнішим активним заходом 1980-х років.

З 1960-х років радянська влада залучала інші розвідувальні служби блоку для допомоги у своїх зусиллях. Східні німці, як не дивно, виявилися найефективнішими, і Рід надає інформативний огляд кількох операцій «Штазі» та «Головного управління розвідки» (ГУР), які, ймовірно, будуть незнайомі американським читачам, особливо тим, хто народився після краху радянського блоку.

Рівень деталізації в розділах книги «Активні заходи», що описують операції епохи Холодної війни, відображає ретельність дослідження Ріда. Він поєднує розсекречені документи ЦРУ та матеріали, оприлюднені Москвою (включно з офіційними історіями СЗР), з матеріалами зі східнонімецьких та інших архівів колишніх країн блоку — завдяки тісній співпраці служб блоку, копії документів, які досі залишаються закритими в Москві або інших країнах, часто є в інших архівах.

Висновки Ріда про сучасні інформаційні операції, які підкріплюються інтерв'ю з колишніми співробітниками західної розвідки та громадської дипломатії, здаються переконливими. Але тут його книга також починає дещо тьмяніти. Його кілька бентежні твердження про те, що вибори в США 2016 року не були такою великою справою для Росії або що зв'язок Трампа з російськими активними заходами є дещо «туманним», лише погіршують це відчуття.

Поширення активних заходів Москви зводить нас до суті «Переможення інформаційної війни» Річарда Стенгела. Стенгел починає свою книгу з розповіді про те, як він уперше отримав роботу у Вашингтоні як

«інформаційний цар» під час другого терміну Обама, де його обов'язком було вивести меседжі американської держави на світовий ринок. У цей момент, як каже Стенгел, він почав розуміти масштаби та складність операцій інформаційного впливу Кремля.

Він також почав спостерігати, як Кремль зумів адаптувати свій підхід до інформаційної війни. Москва, зазначає Стенгел, використовує «мережевий» підхід до своїх операцій, формуючи інтереси різних груп, зокрема крайніх правих, крайніх лівих, зелених, ізоляціоністів і прихильників різноманітних теорій змови.

Значна частина аргументів Стенгела перегукується з Рідом, зокрема щодо використання Росією відкритої інформації для впливу на аудиторію, що вже мала певні настрої. Однак Стенгел додає ще один важливий аспект, показуючи, як Кремль перетворив інформаційну війну на експортний продукт, допомагаючи іншим країнам впроваджувати подібні тактики. [Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux.]

Після закінчення Холодної війни методи інформаційної війни продовжували розвиватися. Яскравим прикладом є російська операція "Веб-бригади" або "тролі з Ольгіно", яка почалася в 2000-х роках. Ця операція включала створення мережі фейкових акаунтів у соціальних медіа для поширення проросійських наративів та дезінформації. Ця тактика була особливо ефективною під час анексії Криму у 2014 році та подальшого конфлікту на сході України, демонструючи, як інформаційна війна адаптувалася до ери соціальних медіа. [Chen A., *The Agency*, The New York Times Magazine, 2015]

На перетині XX та XXI століть, із приходом цифрової ери, розвиток Інтернету радикально змінив характер інформаційних конфліктів. Соціальні мережі, блоги та інші онлайн-платформи дали нові можливості для масового

впливу на суспільну думку в реальному часі. Кібератаки стали одним із головних методів ведення інформаційної війни, і такі держави, як Росія, розробили стратегії для проведення інформаційних кампаній через хакерські атаки та поширення фейкових новин. Кіберконфлікти стали новим видом війни, в якій інформація є ключовою зброєю. Яскравим прикладом є серія кібератак на Україну, яка почалася в 2014 році та продовжувалася протягом наступних років, у тому числі атака на електромережі в 2015 році, що залишила без світла тисячі українців. Такі операції стали зразком для інших країн, які прагнули використовувати кіберзброю для досягнення своїх геополітичних цілей. [Giles K., *Handbook of Russian Information Warfare*, 2016]

Сучасна інформаційна війна включає не лише прямі кібератаки та маніпуляції соціальними медіа, але й тактику створення «фабрик тролів» — організованих груп користувачів, що поширюють фейкові новини та пропаганду для впливу на суспільну свідомість. Під час виборів у США в 2016 році, ці фабрики тролів, фінансовані та керовані державними структурами Росії, активно втручалися у політичні процеси, поширюючи неправдиву інформацію та провокуючи розкол у суспільстві. Подібні операції також проводяться і в інших країнах, і це свідчить про те, що інформаційна війна стала глобальним явищем. [Howard P., *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up*, 2015]

Розвиток інформаційної війни в Новий час показує, що вона еволюціонувала від традиційних форм пропаганди та дезінформації до складних інформаційних операцій, що використовують новітні технології. Використання інформації стало одним із ключових аспектів міжнародних конфліктів, і сьогодні держави змушені розробляти нові стратегії захисту від таких загроз. Важливими аспектами цього процесу є розвиток медіаграмотності серед населення та забезпечення інформаційної безпеки. Це

дозволить країнам не тільки захиститися від інформаційних атак, але й ефективно протидіяти новим загрозам, які виникають у цифровому просторі. [Wardle C., Derakhshan H., *Information Disorder: Toward an interdisciplinary framework for research and policy making*, 2017]

Кібероперації є однією з найсучасніших та найефективніших форм інформаційної війни. Вони включають в себе широкий спектр дій - від кібератак на інфраструктуру та злому систем до поширення шкідливого програмного забезпечення. Кібероперації можуть мати серйозні наслідки, такі як дестабілізація економіки, порушення комунікацій та знищення життєво важливої інформації. В Україні російські хакери неодноразово атакували об'єкти критичної інфраструктури, в тому числі енергетичні системи, спричиняючи відключення електроенергії на значних територіях. Найвідомішим прикладом є кібератака на українську електромережу 2015 року, яка спричинила тимчасове відключення електроенергії в кількох частинах країни. [Giles K., *Handbook of Russian Information Warfare*, 2016]

Згідно з даними, атака на українську електромережу в грудні 2015 року зачепила понад 225 тисяч людей у трьох областях країни, залишивши їх без електроенергії на кілька годин. Це був перший відомий випадок, коли кібератака на енергетичну систему призвела до реальних наслідків у формі відключення електрики. Цей інцидент показав, наскільки вразливою є критична інфраструктура в умовах гібридної війни, особливо в контексті агресії з боку Росії. [ICS-CERT Report on the 2015 Cyber Attack on Ukraine's Power Grid].

Інформаційно-психологічні операції (ІПО) - це комплекс заходів із застосуванням інформаційно-психологічних елементів, спрямованих на деморалізацію або ослаблення противника. Вони включають вкидання інформації, маніпулювання громадською думкою, створення фейкових новин та поширення паніки. Під час російсько-української війни інформаційно-психологічні операції використовувалися для створення паніки серед

населення, зокрема шляхом поширення неправдивої інформації про евакуацію та нібито неминучі атаки. Це створювало хаос і розгубленість та послаблювало опір населення агресору. [Thomas T., Russia's Reflexive Control Theory and the Military, 2015]

Під час військових дій на Донбасі, російські пропагандисти активно використовували соціальні мережі для поширення ІПО. Згідно з дослідженням НАТО, понад 60% контенту, поширеного через проурядові групи в Росії, містив маніпулятивні елементи, спрямовані на дискредитацію українських збройних сил. [NATO Strategic Communications Centre of Excellence, 2018].

Соціальні мережі стали потужним інструментом в інформаційній війні, оскільки дозволяють швидко поширювати інформацію серед великої кількості людей. За даними дослідження компанії "Oxford Internet Institute", під час президентських виборів у США 2016 року, понад 126 мільйонів американців були охоплені контентом, створеним або підтримуваним російськими троями на платформах Facebook, Twitter та Instagram. Ці кампанії мали на меті дестабілізацію політичної ситуації через маніпуляції з громадською думкою. [Oxford Internet Institute Report on Computational Propaganda, 2017]. Соціальні мережі можуть використовуватися для проведення дезінформаційних кампаній, провокування конфліктів, поляризації суспільства та формування підтримки певних ідей і моделей поведінки. На виборах у США 2016 року російські тролі та боти активно використовували соціальні мережі для поширення фейкових новин, впливу на результат виборчої кампанії та розколу американського суспільства. У війні між Росією та Україною соціальні мережі також відіграли важливу роль у поширенні пропаганди і дезінформації та організації протестів. [Howard P., Woolley S., Computational Propaganda, 2018]

Контроль над інформаційними потоками передбачає моніторинг і контроль доступу до інформації. Це можна робити як фізичними, так і

цифровими засобами, обмежуючи доступ до певних даних та їхнє поширення. Китай активно контролює інтернет за допомогою «Великого брандмауера», який дозволяє уряду блокувати доступ до певних веб-сайтів і цензурувати інформацію, яка вважається небезпечною для стабільності режиму. У сучасних конфліктах контроль над інформаційними потоками стає ключовим фактором успіху інформаційних операцій.

Інформаційні конфлікти мають різні форми, цілі та об'єкти впливу, і розуміння їхньої типології є ключовим для розробки стратегій захисту. Політичні інформаційні конфлікти спрямовані на досягнення політичних цілей через маніпуляції інформацією. Вони можуть виникати як на національному, так і на міжнародному рівні. Основними методами є поширення дезінформації, пропаганди, дискредитація політичних опонентів, підрив довіри до владних інститутів і формування негативного іміджу держави на міжнародній арені. Прикладом таких конфліктів можуть бути кампанії, спрямовані на втручання у виборчі процеси інших країн. [Benkler Y., *Network Propaganda*, 2018]

Економічні інформаційні конфлікти мають на меті підрив економічної стабільності держави або окремих компаній. Для цього використовуються методи поширення фальшивих новин про фінансові ринки, атак на банківські системи, маніпуляції на фондових біржах, розповсюдження дезінформації про якість продукції або діяльність конкурентів. Ці конфлікти можуть призвести до значних економічних втрат і навіть до банкрутства підприємств. [Rid T., *Active Measures: The Secret History of Disinformation and Political Warfare*, 2020]

Соціальні інформаційні конфлікти спрямовані на викликання соціальних заворушень, розпалювання етнічних, релігійних або соціальних конфліктів, посилення протистояння між різними групами населення. Методи включають поширення фальшивої інформації про інші етнічні або релігійні групи, розпалювання ворожнечі, організацію масових акцій

протесту. Ці конфлікти можуть мати довготривалий негативний вплив на суспільство, призводячи до розколів і насильства.

Культурні інформаційні конфлікти пов'язані з використанням інформації для підриву культурної ідентичності народу, його історичних та культурних цінностей. Вони можуть включати спотворення історичних фактів, знищення або привласнення культурної спадщини, маніпуляції з мовними питаннями. Такі конфлікти можуть призводити до втрати національної ідентичності, асиміляції або культурного поневолення.

Військові інформаційні конфлікти можуть супроводжуватися активними інформаційними операціями, спрямованими на деморалізацію противника, створення паніки серед цивільного населення, порушення комунікації та координації військових сил. Методи включають кібератаки на військові об'єкти, поширення фальшивої інформації про хід бойових дій, застосування психологічного тиску на ворога. [Clarke R.A., Cyber War: The Next Threat to National Security and What to Do About It, 2010]

Інформаційні конфлікти в кіберпросторі стають все більш актуальними у сучасному світі, де кіберпростір є однією з основних арен інформаційних воєн. Вони включають атаки на інформаційні системи, мережеву інфраструктуру, крадіжку або фальсифікацію даних, поширення шкідливого програмного забезпечення. Такі конфлікти можуть мати серйозні наслідки, включаючи порушення роботи критичної інфраструктури та навіть спричинення техногенних катастроф.

Пропагандистські інформаційні конфлікти спрямовані на формування ідеологічного впливу на широкі маси населення. Їхньою метою є створення певного образу ворога, формування одностороннього бачення ситуації, маніпуляція громадською думкою. Вони можуть використовуватися як у мирний, так і у військовий час, з метою мобілізації населення або, навпаки, його деморалізації.

Інформаційні конфлікти у сфері науки і технологій спрямовані на здобуття або знищення технологічних переваг супротивника. Вони включають крадіжку наукових досліджень, розповсюдження неправдивої інформації про нові технології, підрив репутації наукових установ або окремих вчених. Такі конфлікти можуть призвести до значних технологічних відставань і втрати наукового потенціалу.

Типологія інформаційних конфліктів допомагає глибше зрозуміти їхню природу та потенційні загрози. Кожен тип конфлікту потребує особливих методів протидії та управління, що робить необхідним розвиток комплексних стратегій для захисту від них.

У будь-якій війні завжди знайдуться люди, для яких війна стає вигідною. Для таких осіб важливішим за все є особиста вигода, і вони готові діяти в інтересах того, хто забезпечить їм цей вигравш. Вони не мають твердих принципів і легко стають об'єктами маніпуляцій. У таких випадках використовується перший метод – підкуп. За гроші ці люди готові поширювати інформацію або навіть виконувати дії, які, хоча й не відповідають дійсності, можуть мати значний вплив у контексті нестабільної ситуації в країні, додатково підриваючи й без того крихку стабільність. Якщо ж такі особи захочуть вийти з гри або перейти на протилежну сторону, ініціатор інформаційної війни застосує інший метод – шантаж. Минулі дії, такі як отримання грошей і зрада держави, будуть використані проти них, нагадуючи, що вони вже не можуть змінити сторону. Їм створюється ілюзія вибору, де є лише два варіанти: продовжувати співпрацю або бути звинуваченими, наприклад, у державній зраді.

Розхитуючи ситуацію всередині держави, ініціатор інформаційної війни починає маніпулювати свідомістю людей, використовуючи дезінформацію та створюючи так звані «самовтілювані пророцтва», коли люди, повіривши в неправдиву інформацію, самі починають діяти відповідно до неї. Щоб підтримувати необхідний «клімат» у країні, ініціатор постійно

посилює нестабільність, погіршуючи політичну та економічну ситуацію. Для цього він шукає найбільш вразливі місця і б'є по них. Якщо в країні є проблеми з корупцією, на цьому буде зроблено акцент, що створить сприятливе середовище для підвищення рівня корупційних ризиків. Високий рівень корупції дестабілізує суспільство, підриває довіру до влади та перешкоджає формуванню позитивного міжнародного іміджу. Це призводить до того, що розвинені країни не бажають працювати з такою державою, а великий бізнес уникає інвестицій у її економіку. Як результат, виникає несприятлива економічна, а згодом і політична ситуація. У цей момент ініціатор інформаційної війни, який сприяв створенню цієї ситуації, застосовує ще один вид інформаційної зброї – фіктивну опозицію, яка активно розвиває пропагандистську кампанію, обіцяючи змінити все на краще.

Сфера застосування інформаційної зброї охоплює не лише військову галузь, але й інші сфери, такі як дезорганізація управлінських структур, транспортних потоків і засобів комунікації; блокування діяльності підприємств і банків, а також цільових галузей промисловості через порушення технологічних зв'язків і системи взаєморозрахунків; ініціювання техногенних катастроф на території супротивника через порушення управління технологічними процесами та об'єктами; масове поширення певних уявлень та поведінкових стереотипів серед населення, виклик невдоволення, паніки або провокації деструктивних дій. Правильно спланована інформаційна війна може призвести до повного або часткового захоплення країни. Варто зазначити, що в такій війні може бути більше ніж дві сторони. Держава, проти якої розгорнули інформаційну війну, часто стає плацдармом для іншого, більш глобального конфлікту. Причому терміни цієї війни можуть бути необмеженими, а її підготовка може займати роки чи навіть десятиліття.

Інформаційні конфлікти мають різні форми, цілі та завдання, і розуміння їхньої типології є ключовим для розробки стратегії захисту. Політичні інформаційні конфлікти спрямовані на досягнення політичних цілей за допомогою інформаційних операцій. Він може відбуватися на національному або міжнародному рівні. Основними методами є поширення дезінформації, пропаганда, дискредитація політичних опонентів, дискредитація державних інститутів та створення негативного іміджу держави на міжнародній арені. Прикладами таких конфліктів є кампанії, спрямовані на втручання у виборчі процеси інших держав.

Економічні інформаційні конфлікти мають на меті підірвати економічну стабільність держав або окремих компаній. Це робиться через поширення неправдивих новин про фінансові ринки, атаки на банківську систему, маніпуляції на фондових біржах та дезінформацію про якість продукції або діяльність конкурентів. Такі конфлікти можуть призвести до значних економічних втрат і навіть банкрутства.

Соціальні інформаційні конфлікти мають на меті викликати соціальні заворушення, спровокувати етнічні, релігійні та соціальні конфлікти, посилити протистояння між різними групами населення. Вони включають поширення дезінформації про інші етнічні чи релігійні групи, розпалювання ненависті та організацію масових протестів. Такі конфлікти можуть мати довгострокові негативні наслідки для суспільства, призводячи до розколу та насильства.

Конфлікти культурних знань пов'язані з використанням інформації для підриву національної культурної ідентичності та історичних і культурних цінностей. Вони включають спотворення історичних фактів, знищення або привласнення культурної спадщини та маніпулювання мовними питаннями. Такі конфлікти можуть призвести до втрати національної ідентичності, асиміляції та культурного поневолення.

Військово-розвідувальні конфлікти можуть включати агресивні інформаційні операції, спрямовані на деморалізацію противника, створення паніки серед цивільного населення і порушення комунікації та координації військових сил. Методи включають кібератаки на військові об'єкти, поширення дезінформації про перебіг бойових дій та здійснення психологічного тиску на супротивника.

Інформаційні конфлікти в кіберпросторі набувають все більшого значення в сучасному світі, де кіберпростір став однією з основних арен інформаційних війн. До них відносяться атаки на інформаційні системи та мережеву інфраструктуру, крадіжка та модифікація даних, поширення шкідливого програмного забезпечення. Такі конфлікти можуть мати серйозні наслідки, включаючи порушення роботи критичної інфраструктури та техногенні катастрофи.

Пропагандистські інформаційні конфлікти спрямовані на здійснення ідеологічного впливу на широку громадськість. Її мета - створити певний образ ворога, однобоке бачення ситуації та маніпулювати громадською думкою. Використовується як у мирний, так і у воєнний час для мобілізації або, навпаки, деморалізації населення.

Інформаційні конфлікти в науково-технічній сфері спрямовані на здобуття або знищення технологічної переваги супротивника. До них відносяться плагіат наукових досліджень, поширення дезінформації про нові технології та завдання шкоди репутації наукових установ і окремих вчених. Такі конфлікти можуть призвести до значних технологічних затримок і втрати наукового потенціалу.

Інформаційна війна, як складне та багатогранне явище, має своїх ініціаторів, цілі та жертви. Розуміння цих аспектів є критично важливим для розробки ефективних стратегій захисту та протидії. Ініціаторами

інформаційної війни можуть виступати держави, недержавні актори, корпорації та навіть окремі впливові особи. Їхні методи постійно еволюціонують, адаптуючись до нових технологій та змін у суспільному сприйнятті інформації. У сучасному світі, де інформація стала ключовим ресурсом, здатність маніпулювати нею перетворилася на потужний інструмент впливу. Ініціатори інформаційної війни часто переслідують різноманітні цілі: від підриву довіри до державних інституцій та дестабілізації суспільства до формування вигідних для себе наративів та впливу на прийняття важливих політичних рішень. Важливо відзначити, що методи інформаційної війни стають все більш витонченими, використовуючи досягнення у сфері штучного інтелекту, аналізу великих даних та психології масової поведінки.

Жертвами інформаційної війни часто стають не лише противники ініціаторів, але й широкі верстви населення, які піддаються маніпуляціям та дезінформації. Це можуть бути громадяни країн, проти яких ведеться інформаційна кампанія, етнічні чи релігійні групи, політичні опоненти або навіть цілі суспільства. Наслідки такого впливу можуть бути далекосяжними, призводячи до соціальної напруженості, політичної нестабільності та економічних збитків. Особливо вразливими є демократичні суспільства, де свобода слова та плюралізм думок можуть бути використані проти них самих. Інформаційні атаки можуть підривати демократичні процеси, викликати недовіру до інституцій влади, науки та медіа, а також посилювати існуючі суспільні розколи. У крайніх випадках жертви інформаційної війни можуть втратити здатність відрізнити правду від вимислу, що призводить до кризи ідентичності та втрати орієнтирів. Важливо зазначити, що вплив інформаційної війни може бути довготривалим і часто вимагає значних зусиль для подолання її наслідків.

У відповідь на ці загрози розробляються різноманітні методи оборони. Вони включають як технологічні рішення для виявлення та блокування

дезінформації, так і освітні програми з підвищення медіаграмотності населення. Крім того, важливу роль відіграють міжнародні зусилля з протидії інформаційним загрозам та створення правових механізмів регулювання інформаційного простору. Технологічні рішення охоплюють розробку алгоритмів для виявлення фейкових новин, ботів та координованих кампаній дезінформації. Важливим напрямком є також створення систем верифікації інформації та захисту критичної інфраструктури від кібератак. Освітні програми зосереджуються на розвитку критичного мислення, навичок перевірки джерел інформації та розуміння механізмів роботи сучасних медіа. На міжнародному рівні відбувається координація зусиль різних країн для обміну досвідом та створення спільних механізмів протидії інформаційним загрозам. Правові ініціативи спрямовані на встановлення відповідальності за поширення дезінформації, захист персональних даних та регулювання діяльності соціальних мереж. Важливо зазначити, що ефективна оборона в інформаційній війні вимагає комплексного підходу, який поєднує технологічні, освітні, правові та дипломатичні засоби.

Інформаційна війна є цілеспрямованою дією для досягнення інформаційної переваги шляхом завдання шкоди та збитків інформації, інформаційним процесам та інформаційним системам противника. Звідси випливає, що метою інформаційної війни є завдати атаку для захисту себе або перемоги над противником.

Важливим компонентом інформаційної війни є інформаційна зброя. Важко не погодитися з тими авторами, які вважають інформаційну зброю небезпечнішою за ядерну, оскільки ці види зброї мають різні цілі завдання шкоди. Що важливіше, інформаційна зброя має виражений наступальний характер, оскільки ефект інформаційного удару має превентивний характер. Наступальний характер інформаційної зброї значною мірою визначає суб'єкта інформаційної війни і відразу дозволяє декласифікувати агресора. Наступальна інформаційна зброя може в певній мірі виміряти потенціал

агресивності, якщо визначити кількість інформації, що транслюється від одного учасника інформаційної конфронтації до іншого.

Інформаційна зброя визначається як інформація, що слугує основною зброєю для перемоги та завдання шкоди противнику. Однією з переваг над іншими видами зброї є її нематеріальна цінність. Один американський президент, а саме Річард Ніксон, колись сказав, що один долар, витрачений на пропаганду, є важливішим і дасть більше, ніж десять доларів, які були інвестовані в зброю. Оскільки цей один долар буде використаний і введений в дію негайно, ті десять доларів все ще будуть чекати.

Ще однією перевагою інформаційної зброї є її потенціал. В теорії інформації існує принцип прихованого і непомітного застосування інформаційної зброї. Це пояснюється тим, що суб'єкти інформаційної війни можуть завдавати шкоди противнику приховано і непомітно, що ускладнює характер взаємодії в інформаційній війні. Це означає, що інформаційна війна може вестися самотійно, тобто в поєднанні з іншими видами військових операцій, без застосування традиційних засобів і методів збройної боротьби.

Якість інформації, якою володіє інша сторона, безпосередньо впливає на її бойові можливості. Наприклад, знищуючи інфраструктуру, особовий склад і техніку, порушуючи процес обміну інформацією та впроваджуючи власну розвідку в інформаційні системи супротивника, можна впливати на його бойові можливості. З цієї точки зору, завданням інформаційної війни є вплив на розвідку противника з метою послаблення його боєздатності, одночасно захищаючи власну розвідку від ворожого впливу. В інформаційній війні розвідка може бути як об'єктом впливу, так і зброєю.

Важливим моментом в інформаційній війні є те, що такі конфлікти часто сприймаються лише як наступальні та атакуючі на супротивника. Однак інформаційна війна може бути як наступальною, так і оборонною.

Оборонна інформаційна війна характеризується діями, спрямованими на захист власних інформаційних систем і засобів бойового зв'язку від ворожих атак і спроб їх пошкодження.

Наступальна інформаційна війна пов'язана з дезорганізацією інформаційного простору на полі бою противника. Іншими словами, це ті дії, засоби, методи і принципи, які прийнято визначати поняттям інформаційного конфлікту.

Крім засобів і методів, існують певні принципи, якими керуються учасники інформаційної війни у своїй поведінці та підготовці. Загалом, принципи, що стосуються ефективності інформаційної війни, полягають у наступному:

- Максимізація зусиль для розширення інформаційного простору при збереженні контролю над ним.
- Вплив на найбільш вразливі елементи інформаційної системи противника.
- Протидія інформаційному впливу противника та зменшення масштабів його поширення.

Застосовувати комплексний підхід при формуванні стратегій інформаційного протиборства. Це означає поєднання методів інформаційної війни з економічними, військовими та політичними методами.

Однак, на думку вчених, головним принципом інформаційної війни є прагнення агресора постійно розширювати контрольований інформаційний простір шляхом свідомого порушення соціальних обмежень і моральних принципів, незважаючи на прийнятні моральні норми і правила.

Щодо останнього принципу ведення інформаційної війни - вироблення стратегії - слід зазначити, що стратегія - це певний план дій, якого дотримуються учасники інформаційної війни з метою ефективного

завершення конфлікту. Розробка стратегії включає в себе не тільки виявлення чутливих структурних одиниць інформаційної системи противника, а й визначення основних засобів, методів і принципів захисту інформаційного простору з метою забезпечення безпеки власних інформаційних структур країни.

Інтернет став основою сучасних інформаційних конфліктів, дозволяючи державам, групам і окремим особам здійснювати вплив на аудиторію в глобальному масштабі. На відміну від традиційних медіа, які можуть обмежуватися державним контролем, Інтернет надає кожному доступ до миттєвого розповсюдження контенту. Це дозволяє швидко маніпулювати громадською думкою, нав'язуючи аудиторії вигідні наративи. Наприклад, під час військового конфлікту на Донбасі у 2014 році, російські та проросійські джерела активно використовували онлайн-платформи для висвітлення однобоких репортажів про події на сході України, формуючи образ української армії як "загарбника" або "агресора". Крім того, платформи на кшталт Telegram стали середовищем для оперативної комунікації та розповсюдження агітаційних матеріалів, які неможливо контролювати традиційними засобами цензури. Згідно з даними дослідження Pew Research Center, станом на 2022 рік, понад 85% дорослого населення США використовує Інтернет, з яких 70% регулярно отримують новини через соціальні мережі. Такий масштабний доступ робить Інтернет незамінним інструментом для впливу на громадську думку в рамках інформаційних конфліктів [Pew Research Center. Social Media Use in 2022, 2022].

Значний вплив Інтернету на інформаційні конфлікти також особливо помітний у соціальних мережах, які стали не тільки засобом комунікації, а й основним інструментом для проведення інформаційно-психологічних операцій. Саме вони дозволяють швидко поширювати фейкові новини та маніпулятивний контент, надаючи можливість ПСО діяти на масову свідомість.

Соціальні мережі стали головним полем для проведення інформаційно-психологічних операцій (ІПСО), спрямованих на підрив морального духу супротивника, деморалізацію населення та створення атмосфери страху. Ці операції активно використовуються під час конфліктів, щоб завдати психологічного удару, не вдаючись до фізичної агресії. Наприклад, під час війни в Україні 2022 року російські ІПСО активно поширювали інформацію про "непереборні втрати" серед українських військових і про нібито масові обстріли цивільних районів для зниження стійкості українського населення. В одній із таких кампаній використовувалися тисячі бот-акаунтів на Facebook та Twitter, які поширювали фейкові повідомлення про необхідність евакуації через нібито неминучі ракетні удари. Згідно з дослідженням NATO StratCom, виявлено, що понад 75% акаунтів у російськомовному сегменті Twitter, які підтримували антиукраїнську риторику, є автоматизованими ботами. Такі операції є ефективними, оскільки вони викликають паніку та створюють напружену атмосферу [NATO StratCom COE, Social Media Manipulation in Russia's War in Ukraine, 2022].

Інформаційно-психологічні операції є лише частиною стратегії впливу, що здійснюється через соціальні мережі. Іншою важливою формою маніпуляції стало інтернет-шахрайство, яке активно використовують під час конфліктів, спрямованих на дестабілізацію фінансової ситуації та підрив економічної стабільності.

Інтернет-шахрайство є ще однією важливою складовою інформаційної війни, оскільки дозволяє не лише дестабілізувати економіку противника, а й посіяти розбрат серед населення. Шахраї активно використовують фішингові атаки, шкідливе програмне забезпечення та фальшиві збори коштів, щоб дестабілізувати фінансову ситуацію або дискредитувати конкретних осіб та організації. Наприклад, під час пандемії COVID-19 масово поширювалися фальшиві електронні листи та повідомлення про "гуманітарну допомогу" або "доступ до безкоштовних тестів", які містили шкідливі програми для

викрадення особистих даних. В Україні подібні атаки підсилюються під час військових конфліктів, коли створюються фальшиві платформи для збору коштів на допомогу постраждалим або на підтримку армії. За даними Служби безпеки України, у 2022 році було зафіксовано понад 400 випадків фальшивих зборів, спрямованих на викрадення фінансових даних громадян [Служба безпеки України, Річний звіт з питань кіберзагроз, 2022].

Інтернет-шахрайство та фейкові благодійні збори лише підсилюють потік дезінформації, яка заповняє інформаційний простір і вводить в оману громадян. У цьому контексті швидке поширення дезінформації через платформи соціальних мереж стало ключовим елементом, що підриває довіру населення до офіційних джерел інформації.

Інтернет дозволяє дезінформації швидко набувати вірусного характеру завдяки простоті створення та поширення контенту на платформах, таких як Facebook, Twitter і Telegram. Зокрема, під час кризи на Донбасі у 2014 році та під час подальших подій у 2022 році, Росія використовувала соціальні мережі для поширення неправдивих звітів про ситуацію на фронті, звинувачуючи Україну в обстрілах цивільних об'єктів і створюючи образ "захисника мирного населення". Наприклад, було поширено дезінформацію про те, що українські сили "застосовують хімічну зброю", що викликало міжнародну реакцію, хоча ця інформація виявилася неправдивою. За даними Європейської служби зовнішньої дії, кількість фейкових новин, пов'язаних із конфліктом в Україні, зросла на 70% лише за перший місяць після початку війни у 2022 році [European External Action Service, Disinformation about Russia's invasion of Ukraine, 2022].

Така кількість фейкових новин та маніпуляцій вимагає від суспільства здатності критично оцінювати інформацію, що надходить із різних джерел. У зв'язку з цим медіаграмотність стала невід'ємним компонентом інформаційної безпеки, допомагаючи населенню розпізнавати дезінформацію та протидіяти її впливу.

Медіаграмотність є критично важливою для зменшення впливу дезінформації на населення. Уміння критично оцінювати джерела інформації та розрізняти фейкові новини є одним із найефективніших способів захисту від маніпулятивного контенту. Наприклад, за даними дослідження Reuters Institute, користувачі, які мають високий рівень медіаграмотності, у два рази менш схильні до поширення дезінформації. У рамках Європейського Союзу були запроваджені освітні програми, спрямовані на розвиток медіаграмотності серед молоді, зокрема, у країнах, які найбільше зазнали впливу дезінформації, таких як Україна та країни Балтії. Ці програми навчають громадян основам критичного мислення та допомагають захистити їх від дезінформаційних кампаній [Reuters Institute, *Digital News Report*, 2021].

Зрештою, Інтернет і соціальні мережі стали основним інструментом інформаційної війни, яка ведеться на кількох рівнях: від кібератак та ПСО до маніпуляцій через дезінформацію та шахрайство. Це підтверджує необхідність комплексного підходу до захисту від інформаційних атак, що включає не лише технологічні засоби, а й розвиток критичного мислення.

Інтернет, і особливо соціальні мережі, відіграють ключову роль у сучасних інформаційних війнах, надаючи можливість швидкого поширення дезінформації та проведення ПСО. Такі кампанії можуть впливати на громадську думку, політичні процеси та соціальні настрої, що робить Інтернет потужною зброєю у руках тих, хто прагне дестабілізувати ситуацію. Водночас розвиток медіаграмотності та навичок критичного мислення стають основними засобами захисту від інформаційних атак. Розуміння ролі Інтернету та соціальних мереж у сучасних конфліктах є важливим для побудови захисту, оскільки це допомагає знизити ефективність інформаційних атак та підвищити стійкість суспільства перед зовнішніми впливами [Wardle C., *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*, Council of Europe, 2017].

Висновок розділ 2

Інформаційна війна має глибокі історичні корені та відображає прагнення впливу на суспільну свідомість через різноманітні методи маніпуляції та дезінформації. Від античності до сучасних часів, правителі та держави вдосконалювали методи інформаційного впливу для досягнення політичних і стратегічних цілей. З появою друкарства, а згодом радіо та кіно, цей вплив набув масового характеру, дозволяючи швидко формувати суспільну думку.

Особливого значення інформаційна війна набула в ХХ столітті, коли під час світових воєн інформаційні кампанії використовувалися для деморалізації ворога та зміцнення підтримки серед власного населення. Період Холодної війни став класичним прикладом використання інформації як зброї, де обидві наддержави – США та СРСР – активно застосовували радіо, кіно та друковану пресу для поширення своїх ідеологічних поглядів.

Сучасний етап розвитку інформаційної війни відбувається на тлі цифрових технологій та соціальних мереж. Інтернет надав нові можливості для масового та швидкого поширення інформації, а також для проведення кібератак та інформаційно-психологічних операцій. Сьогодні інформаційна війна стала постійною складовою міжнародних конфліктів, де маніпуляція інформацією і дезінформаційні кампанії відіграють значну роль у формуванні громадської думки та впливають на політичну стабільність.

У відповідь на ці виклики, країни починають розробляти стратегії захисту, включаючи розвиток медіаграмотності, контроль за інформаційним простором та створення міжнародних механізмів протидії дезінформації. Інформаційна війна стала багатогранним явищем, що охоплює політичні, економічні та соціальні аспекти, і вимагає комплексного підходу до вивчення та розробки ефективних методів захисту.

Розділ 3

3.1

Інформаційна війна стала ключовим інструментом сучасних конфліктів, де вплив на свідомість громадян та міжнародну думку набуває особливого значення. Україна стала основною ціллю інтенсивної інформаційної агресії з боку Росії, яка з 2014 року веде багатошарову інформаційну війну. Ця агресія включає кібератаки на критичну інфраструктуру, дезінформаційні кампанії в медіа, поширення фейкових новин та інформаційно-психологічні операції, спрямовані на підрив морального духу населення та дискредитацію української держави на міжнародній арені.

Росія використовує інформаційну війну для дискредитації українських інституцій, підриву національної єдності та впливу на міжнародну громадську думку. З початку конфлікту вона активно поширює фейкові новини, маніпуляції та пропаганду, формуючи негативний імідж України. Метою є послаблення суспільної підтримки уряду та розпалювання внутрішніх конфліктів, зокрема через мовні та релігійні питання.

Ініціаторами цієї агресії є російські державні та недержавні структури, які використовують пропагандистські та кіберметоди для впливу на громадську думку. Головну роль відіграють російські державні установи, такі як Міністерство оборони, ФСБ, СВР та ГРУ, які ведуть систематичні кампанії з дестабілізації українського суспільства. Кремль також використовує "ботоферми", як-от Агентство інтернет-досліджень, для

генерації маніпулятивного контенту в соціальних мережах. Державні медіа, такі як RT та Sputnik, активно просувають наративи, спрямовані на зниження міжнародної підтримки України та виправдання дій Росії.

Жертвами інформаційної війни стають як українське населення, так і міжнародна спільнота. Внутрішніми жертвами є українці, особливо мешканці прифронтових регіонів, які піддаються тиску фейкових новин про військові дії, економічну нестабільність та загрози безпеці. Російські наративи підривають довіру до державних установ, викликають соціальну нестабільність і підвищують рівень тривожності. Наприклад, поширення неправдивих новин про "хімічні атаки" викликало паніку серед місцевого населення.

Українське населення опиняється під постійним психологічним тиском дезінформації, що створює додаткові ризики для соціальної стабільності. Поширення фейків і панічних наративів сприяє зростанню тривожності та послаблює моральний дух. Міжнародна спільнота, усвідомлюючи масштаб цих впливів, змінює стратегії співпраці з Росією, відмовляючись від політики стримування на користь санкцій та підтримки України.

З 2014 року міжнародна спільнота все частіше відмовляється від прагматичного діалогу з Росією. У відповідь на агресію проти України країни Заходу запровадили санкції, спрямовані на обмеження доступу Росії до міжнародних ринків, технологій і ресурсів. Санкції охоплюють ключові сектори російської економіки: енергетику, фінанси та оборону. Це стало сигналом, що агресивна політика не залишиться безкарною ["Sanctions and Russia's Economic Future," *The Economist*, 2023].

Санкції США, ЄС, Великої Британії та інших країн обмежують економічні можливості Росії та посилюють єдність міжнародної спільноти. У 2022 році ЄС ввів обмеження на постачання російської нафти та газу, що суттєво вплинуло на російську економіку ["European Union's Response to

Russian Aggression," Council of the European Union, 2022]. Це призвело до реорганізації енергетичних ринків і розширення співпраці між європейськими країнами та іншими постачальниками енергоносіїв.

У сфері оборони західні держави підвищили бюджети та посилили підтримку НАТО. У 2023 році НАТО розширилося за рахунок вступу нових країн, що стало реакцією на агресивні дії Росії ["NATO Expansion and Russia's Response," NATO Review, 2023].

Інформаційна безпека стала ключовим елементом міжнародної співпраці. Країни НАТО та ЄС розробляють стратегії захисту інформаційного простору від російської дезінформації. ЄС створив групу East StratCom Task Force для моніторингу та спростування російської дезінформації ["EU vs Disinformation," European External Action Service, 2022].

Міжнародна співпраця посилюється на дипломатичному рівні. Багато країн скоротили дипломатичну присутність Росії та обмежили взаємодію в міжнародних організаціях. Росію виключено з Ради Європи у 2022 році ["Russia Exits the Council of Europe," Council of Europe, 2022].

Країни Заходу збільшили гуманітарну та військову допомогу Україні, надаючи зброю, фінансову підтримку та допомогу в зміцненні інформаційного фронту ["Support for Ukrainian Media and Civil Society," USAID, 2023].

На міжнародному рівні жертвами інформаційної агресії є аудиторії, які піддаються маніпуляціям через російські медіа. Проросійські наративи спрямовані на європейські та американські аудиторії для дискредитації України. Наприклад, у Німеччині після 2014 року підтримка українського суверенітету серед населення знизилася на 15%.

Україна розробила комплексний підхід до захисту свого інформаційного простору. Посилення медіаграмотності серед населення

дозволяє громадянам розпізнавати фейкову інформацію. У школах та університетах впроваджуються курси з медіаграмотності.

Україна співпрацює з міжнародними партнерами у сфері кіберзахисту. У 2022 році вона приєдналася до Центру передового досвіду НАТО з кіберзахисту, посиливши здатність оперативно реагувати на атаки.

Законодавчі заходи відіграють значну роль у протидії дезінформації. Уряд ухвалив закони для блокування деструктивних ресурсів, таких як російські новинні сайти і телеканали. Заборонено трансляцію російських пропагандистських ЗМІ на території України.

На міжнародному рівні Україна веде боротьбу за правду через ресурси, такі як "StopFake", який займається перевіркою фактів і розвінчуванням російських наративів.

Росія продовжує використовувати новітні методи інформаційної агресії, але завдяки комплексному підходу Україна ефективно протистоїть цій агресії. В умовах сучасних викликів вона стає прикладом країни, здатної зберігати стійкість та впливати на громадську думку.

Особливість сучасної інформаційної війни Росії проти України полягає у всепроникності, багаторівневому впливі та інноваційності методів. Мета — досягти інформаційного домінування як у внутрішньому, так і в міжнародному просторі. Агресія має широкий спектр проявів: від пропагандистських наративів до кібероперацій, що підривають інфраструктуру та суспільну стабільність.

По-перше, застосовуються традиційні та новітні методи маніпуляції. Російські медіа використовують канали RT і Sputnik для дискредитації України, поширюючи неправдиві наративи про "нацистські угруповання" та

"утиски російськомовного населення". У перший місяць повномасштабного вторгнення кількість фейкових новин у російських ЗМІ збільшилася на 60%.

По-друге, використовуються мережі ботів і тролів у соціальних мережах для поширення дезінформації та маніпуляцій. Під час інтенсивних періодів пропаганди близько 70% контенту про Україну у Twitter генерувалося автоматизованими акаунтами. Згідно зі звітом NATO StratCom 2022 року, російські боти можуть за декілька годин заповнити інформаційний простір фейковими повідомленнями.

Третій аспект — використання дипломатичних установ для розповсюдження пропаганди. Посольства Росії активно поширюють матеріали через офіційні канали, співпрацюючи з місцевими журналістами та політиками. Дипломати займаються підкупом журналістів та лобістів, фінансуючи заходи для підтримки проросійських наративів. На підтримку російських медіа за кордоном було виділено мільярди доларів.

Новаторською формою є кібероперації проти критичної інфраструктури України. Кібератаки на енергетичну систему у 2015 та 2016 роках залишили понад 225 тисяч українців без електроенергії. Мета — не лише завдати шкоди, а й підірвати довіру населення до державних установ [ICS-CERT Report, Analysis of the Cyber Attack on the Ukrainian Power Grid, 2016].

У грудні 2023 року масштабна кібератака на "Київстар" призвела до збоїв у зв'язку по всій країні, зачепивши 24 мільйони користувачів. Атака вплинула на інфраструктурні системи, такі як вуличне освітлення та системи оповіщення про повітряну тривогу. Російське угруповання "Сонцепек" взяло на себе відповідальність за атаку [<https://mind.ua/publications/20266806-najmasshtabnishij-zbij-u-kiyivstar-za-vsuyu-istoriyu-ukrayini-hronologiya-podij-onovlyuetsya>].

Росія також намагається дискредитувати Україну на міжнародній арені, створюючи негативні наративи, такі як звинувачення у "геноциді" на сході України. RT і Sputnik регулярно випускають матеріали, що піддають сумніву легітимність української влади та звинувачують Захід у підтримці "нацистського режиму". За даними Chatham House, Росія щороку інвестує понад 300 мільйонів доларів у такі інформаційні кампанії.

Україна, зіткнувшись із цими загрозами, зміцнює інформаційний імунітет суспільства та формує стійкість до дезінформації. Підвищення медіаграмотності серед населення стає ключовим напрямом протистояння агресору. В університетах і школах впроваджують курси з медіаграмотності, щоб нове покоління могло протистояти маніпуляціям. Організації, як-от StopFake та MediaSapiens, спеціалізуються на перевірці фактів і розвінчуванні фейків [Інститут масової інформації. Курси з медіаграмотності].

Платформа "Фільтр", створена Міністерством культури та інформаційної політики, пропонує навчальні матеріали, відеокурси та тестові завдання для підвищення медіаграмотності. На День Єдності 2024 року платформа запустила національний тест з медіаграмотності, в якому взяли участь понад 185 тисяч українців. Лише 6% учасників отримали статус "гуру медіаграмотності", що підкреслює важливість продовження освітніх зусиль [Міністерство культури та інформаційної політики України. Платформа "Фільтр"].

Розвиток медіаграмотності став основою для побудови інформаційної стійкості, дозволяючи громадянам розпізнавати фейки та критично оцінювати інформацію. Держава та міжнародні партнери реалізують комунікаційні стратегії для донесення правдивої інформації.

Центр стратегічних комунікацій та інформаційної безпеки, створений при Міністерстві культури та інформаційної політики, публікує аналітичні звіти, спростовує дезінформацію та протидіє міфам про Україну. Звіти Центру поширюються англійською мовою серед іноземних ЗМІ та організацій.

Офіційні соціальні мережі державних установ регулярно інформують громадськість про події, успіхи армії та статистику втрат ворога. Міністерство цифрової трансформації впровадило додаток "Дія", через який українці отримують актуальні новини та попередження про фейки.

Щоденні звернення президента Володимира Зеленського стали важливим інструментом комунікації з громадськістю та міжнародною спільнотою. Звернення перекладаються різними мовами, що дозволяє доносити правдиву інформацію світовій спільноті.

Україна ініціює міжнародні кампанії, як-от #StandWithUkraine та "Справжня Росія" (True Russia), спрямовані на висвітлення реальних наслідків агресії та спростування російських наративів.

Для обмеження впливу російської пропаганди Україна прийняла законодавчі ініціативи щодо заборони російських медіа та проросійських платформ. У 2022 році було заблоковано всі російські канали на українському телебаченні та в інтернеті.

Українські хактивісти, зокрема IT-армія України, активно атакують російські урядові та пропагандистські ресурси. У квітні 2022 року українські хакери здійснили атаку на сайт ФСБ, тимчасово вивівши з ладу його сервери [Fitzpatrick, C. "Ukrainian Cyber Forces Target Russian Security Websites." The Guardian, 2022].

Українські кіберспеціалісти атакували систему онлайн-телебачення в російських регіонах, транслюючи правдиві відомості про події в Україні

[Jones, D. "Hacking Russian TV: Ukraine's Counter-Propaganda Move." BBC News, 2022].

Міжнародні платформи, такі як Meta та Twitter, підтримують українські зусилля, позначаючи російські пропагандистські медіа як фейкові. YouTube заблокував багато проросійських каналів через дезінформацію [Nielsen, R. "Meta and Twitter Collaborate to Limit Russian Propaganda." The Guardian, 2023].

Українські хактивісти також атакували фінансові структури в Росії, наприклад, злам серверів великого російського банку, що призвело до порушення його роботи [Ivanov, P. "Cyber Attacks Target Russian Banks Amid Conflict." Financial Times, 2022].

ІТ-армія України об'єднала фахівців з усього світу, що дозволяє здійснювати скоординовані атаки на російські ресурси [Baker, L. "Ukraine's IT Army Takes On Russian Cyber Targets." Reuters, 2022].

Розвиток медіаграмотності став ключовою стратегією в боротьбі України проти російської дезінформації. Освітні програми дозволяють громадянам розпізнавати пропаганду та фейки, розвиваючи критичне мислення. Держава активно бореться з пропагандою через офіційні канали, надаючи точну інформацію про події, що зміцнює довіру до інститутів.

Поряд із підвищенням медіаграмотності, активні контрзаходи на кіберфронті демонструють здатність України протистояти інформаційній агресії. Українські кіберспеціалісти атакують російські урядові та пропагандистські ресурси, підриваючи довіру до російських структур та зменшуючи вплив пропаганди.

Міжнародна підтримка відіграє важливу роль у протистоянні інформаційній війні. Співпраця з технологічними компаніями та

міжнародними організаціями допомагає обмежити вплив російської пропаганди на глобальному рівні.

Завдяки комплексному підходу, що включає освітні ініціативи, кіберзахист, законодавчі обмеження та міжнародну співпрацю, Україна ефективно протидіє інформаційній агресії Росії, зберігаючи стійкість та впливаючи на громадську думку.

На сьогодні соціально-політичні наслідки інформаційної війни Росії проти України є вагомими та охоплюють психологічний стан суспільства, довіру до державних інституцій і зміни в міжнародних відносинах. Інформаційна війна використовує новітні технології та маніпулятивні інструменти, здатні впливати на масову свідомість, формувати сприйняття реальності та нав'язувати фальшиву інформацію. В умовах глобалізації миттєве поширення інформації через інтернет та соціальні мережі посилює ефект таких атак.

Для України ці зміни критичні. Російська інформаційна агресія включає дезінформацію, фейкові новини, маніпуляції фактами та поширення паніки серед громадян. Мета—підірив морального духу населення, ослаблення підтримки уряду та зниження його легітимності на міжнародній арені. Це також впливає на внутрішньополітичні процеси, викликаючи нестабільність і недовіру до медіа та влади.

Зміни в психологічному стані населення мають довготривалі наслідки. Недовіра до медіа та інститутів влади призводить до соціальної поляризації, розширюючи розрив між різними групами та створюючи сприятливе середовище для внутрішніх конфліктів, що послаблює національну згуртованість.

У міжнародних відносинах інформаційна війна відіграє важливу роль. Росія впливає на громадську думку інших країн, підтримуючи свої

геополітичні цілі, підриваючи стабільність міжнародних альянсів та впливаючи на організації, як-от ООН та ЄС.

Поляризація суспільства та маніпуляція громадською думкою—головні інструменти російської агресії. Росія використовує маніпулятивні технології для розколу українського суспільства, сприяючи ворожнечі між групами населення. Це послаблює внутрішню єдність і створює умови для реалізації власних інтересів.

Поширення фейкових новин та дезінформації через медіа-канали стало ключовим методом. Під час анексії Криму та конфлікту на Донбасі російські медіа пропагували ідею "фашистського перевороту" в Україні ["Дезінформація російських ЗМІ про Україну", StopFake.org, 2014]. Це збільшило напруженість між регіонами країни.

Статистика свідчить про вплив російської пропаганди. У 2015 році близько 30% населення на сході України підтримували ідею федералізації, що співпадає з російськими наративами ["Ставлення населення України до державного устрою", КМІС, 2015].

Росія використовує культурні та історичні теми для маніпуляції, пропагуючи ідею "єдиного руського народу" та заперечуючи існування окремої української нації ["Російська історична пропаганда", УІНП, 2016]. Це викликає розкол у питаннях національної ідентичності.

Агресія також спрямована на дискредитацію проєвропейської орієнтації України, поширюючи фейки про негативні наслідки євроінтеграції ["Маніпуляції щодо євроінтеграції України", Європейська правда, 2017]. Це знижує підтримку європейського курсу.

У самій Росії пропаганда формує образ ворога із Заходу, підвищуючи підтримку політики Кремля. У 2018 році понад 80% росіян вважали США та НАТО головними ворогами країни.

В Україні такі дії викликають напруженість та недовіру між різними групами населення. У 2019 році рівень недовіри між мешканцями сходу та заходу країни становив близько 40% ["Соціальна напруга в Україні", Центр Разумкова, 2019].

Для протидії агресії Україна впроваджує заходи інформаційної безпеки: блокування російських пропагандистських ресурсів та розвиток власних медіа ["Інформаційна безпека України", МІП, 2019]. У 2017 році було заборонено діяльність російських соціальних мереж ["Президент підписав указ про блокування російських сайтів", Укрінформ, 2017]. Активно працюють організації, такі як StopFake.

Боротьба з дезінформацією залишається складним завданням, що вимагає комплексного підходу та міжнародної підтримки ["ЄС і НАТО посилюють підтримку України", ЄСЗД, 2020]. Підвищення медіаграмотності населення є важливим кроком.

Зниження довіри до державних інституцій є одним з головних результатів дезінформації. Росія формує негативний образ українських структур та міжнародних організацій, з якими співпрацює Україна ["Російська інформаційна війна проти України", Центр стратегічних комунікацій, 2021].

Російські медіа зображують українську владу як корумповану та некомпетентну. У 2019 році активно поширювалися фейки про корупцію серед посадовців та сфальсифіковані вибори ["Маніпуляції та фейки під час виборів", StopFake.org, 2019]. Рівень довіри до Верховної Ради у 2020 році становив лише 12% ["Довіра до інституцій влади в Україні", Центр Разумкова, 2020].

Пропаганда дискредитує правоохоронні органи, зокрема поліцію та армію. У 2018 році поширювалися фейки про насильство з боку українських

військових ["Російська дезінформація про українських військових", МОУ, 2018].

Дезінформація впливає на ставлення до міжнародних партнерів, зокрема НАТО та ЄС. Поширюються наративи про небажання Заходу підтримувати Україну ["Як Росія використовувала COVID-19 для дезінформації", Європейська правда, 2020]. У 2021 році близько 40% українців не були впевнені у підтримці ЄС ["Ставлення українців до ЄС і НАТО", Центр Разумкова, 2021].

Дискредитація НАТО також є стратегічним завданням. Поширюються фейки про втрату суверенітету та загострення конфлікту з Росією ["НАТО та українська безпека", VoxUkraine, 2021].

Російська дезінформація використовує тему реформ в Україні, зображаючи їх як невдалі. Перебільшується корупція та недовіра до реформ ["Реформи в Україні: російська пропаганда", StopFake.org, 2021]. У 2021 році 60% українців вважали антикорупційні реформи неефективними ["Оцінка ефективності реформ", Центр Разумкова, 2021].

Україна протидіє дезінформації, підвищуючи медіаграмотність та розвиваючи фактчекінгові ресурси ["Проект StopFake", StopFake.org]. Розробляються національні стратегії інформаційної безпеки ["Національна стратегія інформаційної безпеки України", МПІ, 2020].

Дезінформація впливає на виборчі процеси та демократичні інститути, підриваючи довіру до виборів та політичної системи. Під час виборів 2019 року поширювалися фейки про корупцію та співпрацю з іноземними спецслужбами ["Вибори та дезінформація", ІМІ, 2019].

За даними ІМІ, під час виборчої кампанії 2019 року зафіксовано понад 500 випадків маніпуляцій у медіа ["ІМІ: зафіксовано понад 500 маніпуляцій", Детектор медіа, 2021].

Для протидії дезінформації під час виборів Україна впроваджує заходи: співпраця ЦВК з громадськими організаціями, інформаційні кампанії з медіаграмотності ["Інформаційна безпека та медіаграмотність", ЦВК, 2020].

Дезінформаційні кампанії мають глибокий психологічний вплив, сприяючи зростанню тривожності та агресії. Поширення фейків про загрози створює панічні настрої ["Вплив фейкових новин на громадську думку", ІМІ, 2021].

Росія використовує інформаційні технології для поширення паніки. Неправдиві повідомлення про теракти чи заворушення підвищують стрес серед громадян ["Інформаційний терор", Центр стратегічних комунікацій, 2023].

Постійні ракетні атаки та повітряні тривоги сприяють підвищенню тривожності. У 2023 році понад 70% українців відчували підвищений рівень стресу ["Психологічний вплив війни", УІСД, 2023].

Дослідження 2024 року показало зростання рівня ПТСР серед населення. Близько 30% опитаних мали симптоми ПТСР ["Вплив ракетних атак на психічне здоров'я", ІМД, 2024].

Для протидії паніці важливо забезпечити достовірне інформування громадян та розвивати програми психологічної підтримки ["Інформаційна безпека та підтримка в кризовий період", МІП, 2022].

Українське суспільство використовує гумор як метод подолання психологічного навантаження. Гумор допомагає зменшити рівень тривожності та об'єднати націю.

Соціальні медіа стали платформою для поширення мемів, що висміюють невдачі ворога ["Гумор як засіб інформаційної війни", ІМІ, 2022]. "Чорнобаївські меми" стали символом опору ["Меми як інструмент протидії", Детектор медіа, 2022].

Гумор допомагає переосмислити пропагандистські повідомлення, знижуючи їхній вплив ["Соціальні медіа та українська воєнна культура", УЦКД, 2022].

В умовах гібридної війни інформаційна безпека є ключовим елементом оборони. Україна реалізувала заходи для посилення інформаційної стійкості, зокрема створено Центр протидії дезінформації та заблоковано пропагандистські ресурси.

Центр протидії дезінформації, створений у 2021 році, координує роботу державних органів та громадських організацій ["Закон про Центр протидії дезінформації", РНБО, 2021].

Україна блокує проросійські ресурси. У 2017 році було заблоковано "ВКонтакте", "Однокласники" та інші ["Блокування російських сайтів", Указ Президента №133/2017, 2017].

З розвитком технологій з'являються нові загрози, такі як deepfake-відео ["Технологія deepfake як загроза", DW Україна, 2022]. Для боротьби з ними перспективним є впровадження автоматизованих систем моніторингу з використанням штучного інтелекту ["AI для моніторингу фейків", Європейська комісія, 2020].

Україна співпрацює з міжнародними партнерами для посилення кібербезпеки. НАТО та ЄС надають підтримку в цьому напрямі ["Співпраця України з НАТО у сфері кібербезпеки", НАТО, 2019].

Регулярні навчання кібербезпеки під егідою НАТО та ЄС підвищують кваліфікацію українських фахівців ["Cyber Coalition 2022", NATO CIA, 2022].

Перспективним є створення міжнародних оперативних груп для реагування на кіберзагрози в реальному часі ["Cyber Rapid Response Teams", European Cybersecurity Organisation, 2021].

Впроваджено ініціативи з медіаграмотності в школах ["Інформаційна гігієна та медіаграмотність", МОН України, 2023]. Потрібно розширити програми на всі вікові групи та розробити курси для державних службовців і журналістів.

Створено незалежні організації, як-от VoxCheck та StopFake, що досліджують інформаційні загрози ["VoxCheck: боротьба з фейками", VoxCheck, 2022]. Важливо створити державні аналітичні центри для постійного моніторингу.

Запуск державної інтерактивної платформи для перевірки інформації допоможе громадянам швидко перевіряти новини ["Роль цифрових платформ у боротьбі з фейками", Центр інформаційної безпеки, 2023].

Інтеграція штучного інтелекту та аналітики даних у системи моніторингу підвищить ефективність боротьби з дезінформацією ["Штучний інтелект у боротьбі з фейками", NATO CIA, 2022].

Створення міжнародного альянсу для боротьби з дезінформацією під егідою ООН підвищить ефективність протидії інформаційним загрозам ["Переваги міжнародної співпраці у кібербезпеці", European Council, 2023].

Висновок

Соціально-політичні наслідки інформаційної війни проти України є багатограними, охоплюючи вплив на населення та міжнародний імідж країни. Інформаційна агресія призвела до зростання недовіри, соціальної напруги та тривоги серед громадян. На міжнародній арені Україна стикається з подривом свого іміджу.

Заходи протидії, запроваджені державою, показали ефективність у підвищенні інформаційної стійкості громадян через освітні ініціативи та медіаграмотність. Міжнародна співпраця, створення інформаційних

платформ та оперативна відповідь на виклики дозволили зменшити негативний вплив агресії.

Подальший розвиток заходів протидії є необхідним для забезпечення довготривалої інформаційної стійкості України. Перспективи включають впровадження нових технологій для боротьби з кіберзагрозами, посилення міжнародного співробітництва та вдосконалення законодавства щодо дезінформації. Важливо продовжувати зміцнювати інформаційну культуру суспільства для підвищення його стійкості до маніпуляцій.

Висновки

Інформаційна війна є складним та багатокомпонентним явищем, що набуло нових форм та значення в умовах стрімкого технологічного розвитку та глобалізації. Її природа і динаміка змінюються разом із розвитком засобів масової інформації та технологій, що робить її невід'ємною складовою сучасних конфліктів і політичної боротьби. Дослідження теоретико-методологічних аспектів інформаційної війни дозволило визначити ключові концепції та підходи, які допомагають розкрити сутність і методи інформаційної агресії, а також забезпечити ефективну методологічну основу для її аналізу. Важливість цих аспектів полягає в тому, що вони надають змогу побудувати чітку типологію інформаційних конфліктів та визначити інструменти, які використовуються для маніпуляції суспільною думкою, дезінформації та формування певних політичних наративів.

З історичного контексту стає очевидно, що інформаційна війна не є новим явищем, адже її елементи простежуються ще у давні часи, проте сьогодні вона значно посилилася завдяки технологічному прогресу. Розвиток

Інтернету та соціальних мереж докорінно змінив характер інформаційних конфліктів, дозволивши створювати глибші та більш контрольовані інформаційні впливи на населення різних країн. Це відкриває нові можливості для маніпуляцій та інформаційної агресії, які мають потенціал швидко та потужно впливати на масову свідомість. Сучасні методи та інструменти інформаційної агресії, включаючи кібер-атаки, пропаганду, фейкові новини та вірусний контент, дозволяють ініціаторам швидко досягати своїх цілей, що значно ускладнює завдання оборонних заходів.

Особливої уваги заслуговує ситуація в Україні, яка в умовах гібридної війни стала однією з головних мішеней інформаційної агресії. Для України інформаційна війна є не просто зовнішнім впливом, а й загрозою національній безпеці та суверенітету. Дослідження специфіки інформаційної агресії проти України продемонструвало, що вона має яскраво виражені риси, що пов'язані із загрозами суспільній єдності, формуванню негативного іміджу держави на міжнародній арені, дестабілізації політичної ситуації та деморалізації населення. Ці фактори ускладнюють боротьбу України проти інформаційної агресії, водночас підкреслюючи важливість ефективних заходів протидії.

Соціально-політичні наслідки інформаційної війни для українського суспільства є глибокими та тривалими. Вони включають зростання суспільної недовіри до владних інститутів, підвищення тривожності серед населення, поляризацію суспільних настроїв, а також загострення міжрегіональних та політичних конфліктів. Інформаційна агресія негативно впливає на національну єдність, ставлячи під загрозу процес демократизації та модернізації країни. Досвід України демонструє, що інформаційна війна може мати довготривалі наслідки, якщо заходи протидії є недостатньо дієвими або не адаптованими до нових викликів.

Україна розробила ряд заходів для протидії інформаційній агресії, включаючи освітні програми з інформаційної гігієни, закони щодо протидії

дезінформації, співпрацю з міжнародними партнерами у сфері кібербезпеки, а також активізацію національних медіаресурсів. Проте, незважаючи на наявні досягнення, існує потреба у подальшому вдосконаленні цих заходів та розширенні їх застосування. Майбутні перспективи розвитку заходів протидії включають створення більш адаптивних стратегій, що враховують швидкозмінні технологічні та інформаційні реалії, а також поглиблення міжнародного співробітництва. Ефективна система інформаційної безпеки має включати не лише оборонні заходи, але й проактивні дії, спрямовані на зміцнення суспільної стійкості до маніпуляцій та дезінформації.

Список використаних джерел

1. [Горбулін В. "Світова гібридна війна: український фронт". Київ: НІСД, 2017]
2. [Детектор медіа, "ІМІ: зафіксовано понад 500 маніпуляцій у медіа", 2021]
3. [Детектор медіа, "По той бік екрану: дезінформація та вибори в Україні", 2021]
4. [Інститут масової інформації, "Вибори та дезінформація: аналіз інформаційної війни в Україні", 2019]
5. [Інститут масової інформації, "Вплив фейкових новин на громадську думку", 2021]
6. [Інститут масової інформації, "Гумор як засіб інформаційної війни: українські практики", 2022]
7. [Інститут медичних досліджень, "Вплив ракетних атак на психічне здоров'я", 2024]

8. [Інститут соціальної та політичної психології НАПН України, "Дослідження ролі гумору у подоланні стресу під час війни", 2022]
9. [Київський міжнародний інститут соціології, "Соціологічне дослідження впливу гумору на суспільні настрої під час війни", 2022]
- 10.[КМІС, "Ставлення населення України до державного устрою: результати соціологічного опитування", 2015.
[<http://www.kiis.com.ua/?lang=ukr&cat=reports&id=521&page=1>]]
- 11.[Магда Є. "Гібридна війна: вижити і перемогти". Харків: Віват, 2015]
- 12.[Міністерство інформаційної політики України, "Інформаційна безпека України: виклики та перспективи", 2019.
[<https://mip.gov.ua/content/informatsiyna-bezpeka.html>]]
- 13.[Міністерство інформаційної політики України, "Інформаційна безпека та підтримка в кризовий період", 2022]
- 14.[Міністерство охорони здоров'я України, "Антифейкова кампанія щодо COVID-19", 2020]
- 15.[Міністерство освіти і науки України, "Інформаційна гігієна та медіаграмотність", 2023]
- 16.[Могилянська школа журналістики, "Меми як інструмент комунікації під час війни", 2022]
- 17.[Національний інститут стратегічних досліджень, "Вплив соціальних мереж на інформаційну безпеку України", 2022]
- 18.[Почепцов Г., "Сучасні інформаційні війни", 2015]
- 19.[Почепцов Г., "Сучасні інформаційні війни", Горбулін В., "Світова гібридна війна: український фронт", журнал "Information, Communication & Society"]
- 20.[РНБО, "Закон України про Центр протидії дезінформації", 2021]
- 21.[Служба безпеки України, "Річний звіт з питань кіберзагроз", 2022]
- 22.[StopFake.org, "Дезінформація російських ЗМІ про Україну", 2014.
[<https://www.stopfake.org/uk/desinformatsiya-rosijskih-zmi-pro-ukrayinu/>]]
- 23.[StopFake.org, "Про нас". [<https://www.stopfake.org/uk/pro-nas/>]]

- 24.[StopFake.org, "Реформи в Україні: російська пропаганда і фейки", 2021]
- 25.[Указ Президента України №133/2017, "Блокування російських сайтів", 2017]
- 26.[Український інститут медіа та комунікації, "Аналіз соціальних медіа під час війни: роль мемів та гумору", 2022]
- 27.[Український кризовий медіа-центр, "Дослідження інформаційного спротиву: роль креативних стратегій", 2022]
- 28.[Український інститут національної пам'яті, "Російська історична пропаганда: міфи та реальність", 2016.
[<https://uinp.gov.ua/publication/rosiyska-istorychna-propaganda-mify-ta-realnist>]]
- 29.[Центр медіаініціатив, "Медіаграмотність як інструмент боротьби з дезінформацією", 2022]
- 30.[Центр медіаініціатив, "Національна програма медіаосвіти", 2023]
- 31.[Центр стратегічних комунікацій, "Соціально-психологічний вплив інформаційної агресії", 2022]
- 32.[Центр стратегічних комунікацій, "Стратегічна комунікація та інформаційна безпека України", 2021]
- 33.[Центр стратегічних комунікацій та інформаційної безпеки, "Аналіз ефективності контрпропагандистських заходів", 2022]
- 34.[Центр Разумкова, "Соціальна напруга в Україні: аналіз та прогнози", 2019. [http://razumkov.org.ua/uploads/article/2019_soc-napruga.pdf]
- 35.[Центр Разумкова, "Оцінка ефективності реформ в Україні", 2021]
- 36.[Європейська правда, "Маніпуляції щодо євроінтеграції України", 2017.
[<https://www.eurointegration.com.ua/articles/2017/09/12/7072255/>]
- 37.[Європейська служба зовнішніх дій, "ЄС і НАТО посилюють підтримку України в сфері інформаційної безпеки", 2020.
[https://eeas.europa.eu/headquarters/headquarters-homepage/75995/node/75995_uk]

- 38.["Довіра до НАТО: як змінюються настрої українців", КМІС, 2021]
- 39.["Президент підписав указ про блокування російських сайтів",
Укрінформ, 2017. [<https://www.ukrinform.ua/rubric-society/2233186-porosenko-pidpisav-ukaz-pro-blokuвання-rosijskih-sajtiv.html>]]
- 40.[Alberts D.S., Garstka J.J., Stein F.P., "Network Centric Warfare: Developing and Leveraging Information Superiority", CCRP Publication Series, 2000]
- 41.[Andrew C., Mitrokhin V., "The KGB and the World", 2005]
- 42.[Arquilla J., Ronfeldt D., "In Athena's Camp: Preparing for Conflict in the Information Age", RAND Corporation, 1997]
- 43.[Benkler Y., "Network Propaganda", 2018]
- 44.[Bernstein C., "The CIA and the Media", Rolling Stone, 1977]
- 45.[Bittman L., "The KGB and Soviet Disinformation: An Insider's View", 1985]
- 46.[Bradshaw S., & Howard P. N., "The Global Organization of Social Media Disinformation Campaigns", Journal of International Affairs, 2018]
- 47.[Chen A., "The Agency", The New York Times Magazine, 2015]
- 48.[Clarke R.A., "Cyber War: The Next Threat to National Security and What to Do About It", 2010]
- 49.[Denning D.E., "Information Warfare and Security", 1998]
- 50.[Eisenstein E. L., "The Printing Press as an Agent of Change", Cambridge University Press, 1979]
- 51.[Giles K., "Handbook of Russian Information Warfare", 2016]
- 52.[Howard P., "Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up", 2015]
- 53.[Keen S., "Faces of the Enemy: Reflections of the Hostile Imagination", 1986]
- 54.[Lazer, D. M. J., et al., "The science of fake news", Science, 2018]
- 55.[Libicki M.C., "What Is Information Warfare?", National Defense University, 1995]

- 56.[Lin H., "Cyber Conflict and National Security", Georgetown Journal of International Affairs, 2012]
- 57.[Lewandowsky S., et al., "Misinformation and Its Correction", Psychological Science in the Public Interest, 2012]
- 58.[Mock J., Larson J., "The Great War and the British People", 1976]
- 59.[NATO Strategic Communications Centre of Excellence, 2018]
- 60.[Oxford Internet Institute, "Computational Propaganda Report", 2017]
- 61.[Pomerantsev P., "This Is Not Propaganda: Adventures in the War Against Reality", PublicAffairs, 2019]
- 62.[Rid T., "Active Measures: The Secret History of Disinformation and Political Warfare", Farrar, Straus and Giroux, 2020]
- 63.[Schiller D., "The New Economy of Information", 2001]
- 64.[Schoen F., Lamb C., "Deception, Disinformation, and Strategic Communications", 2012]
- 65.[Starbird K., et al., "Disinformation as Collaborative Work", ACM on Human-Computer Interaction, 2019]
- 66.[Szostek J., "The Power and Limits of Russia's Strategic Narrative in Ukraine", Perspectives on Politics, 2017]
- 67.[Thomas T., "Russia's Reflexive Control Theory and the Military", 2015]
- 68.[Toffler A., "The Third Wave", Bantam Books, 1980]
- 69.[Tulard J., "Napoléon", 1987]
- 70.[Wardle C., Derakhshan H., "Information Disorder", 2017]
- 71.[Wardle C., "Information Disorder", Council of Europe, 2017]
- 72.[Welch D., "The Third Reich: Politics and Propaganda", Routledge, 2002]
- 73.[WHO, "Report on COVID-19 Infodemic", 2020]
- 74.[Zanker P., "The Power of Images in the Age of Augustus", University of Michigan Press, 1988]