МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА

ННІ «Юридичний інститут КНЕУ імені Вадима Гетьмана»
Кафедра політичних технологій

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Політичні технології та лідерство»
галузь знань 05 Соціальні та поведінкові науки
спеціальність 052 Політологія

Форма навчання: очна (денна)

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему: **«ТЕХНОЛОГІЇ ІНФОРМАЦІЙНОЇ ВІЙНИ ТА ЇХ ВПЛИВ НА СУЧАСНІ ПОЛІТИЧНІ ПРОЦЕСИ».**

Здобувачки Бишиньової Олександри Сергіївни _____

Науковий керівник: к.пол.н., доцент, Манелюк Ю.М.

_____

Робота допущена до захисту перед екзаменаційною комісією з атестації здобувачів вищої освіти (ЕК)

Завідувач кафедри: д.пол.н., доцент, Гапоненко В.А.

_____

Київ 2024

ЗМІСТ

ВСТУП **3**

РОЗДІЛ 1 ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ **6**

1.1. Сутність поняття «інформаційна війна» та основні моделі організації інформаційної війни. 6

1.2. Інструменти інформаційної війни та особливості їх реалізації. 11

РОЗДІЛ 2 ФОРМУВАННЯ ТЕХНОЛОГІЙ ІНФОРМАЦІЙНОЇ ВІЙНИ ТА ЇХ ДОСЛІДЖЕННЯ **15**

2.1. Засоби та методи інформаційних війн у світі.

2.2. Сутність «пропаганди» її засоби і механізми як прояв інформаційної війни. 20

2.3. Пропаганда як позитивне явище в контексті формування стратегій державної інформаційної політики. 26

РОЗДІЛ 3 ВПЛИВ ІНФОРМАЦІЙНОЇ ВІЙНИ НА ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ **29**

3.1. Сучасні загрози інформаційній безпеці України під час російсько-українській війні (2014-2024 рр.). 29

3.2. Місце та вплив інформаційної війни в російсько-українській війні (2014-2024 рр.) 35

3.3. Засоби й механізми протидії інформаційній війні для забезпечення інформаційної безпеки в Україні. 35

ВИСНОВКИ **45**

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ **49**

ВСТУП

Актуальність теми. Дослідження технологічних процесів інформаційної війни та її вплив є надзвичайно важливою темою, оскільки Україна перебуває в стані інформаційної війни з росією з 2014 року. Інформаційна війна безпосередньо впливає на політичні процеси, які відбуваються в Україні, зокрема на формування та визначення внутрішньо-політичних процесів та вектору зовнішньополітичних відносин з іншими державами. Щодня громадяни України, навіть не завжди усвідомлюючи цього, є жертвами не тільки повномасштабної війни, яку веде російська федерація проти України, але й жертвами інформаційної війни.

Особливої актуальності окреслена проблематика набуває звичайно після повномасштабного вторгнення російської федерації в Україну 24 лютого 2022 року. У реаліях сьогодення також, коли сучасні інформаційні технології досягли значного розвитку та перебувають на етапі щоденного розвитку та трансформації, інформаційна війна та її сутність, інструменти та методи є об'єктом дослідження багатьох вчених. Повномасштабне вторгнення в Україну 24 лютого 2022 року дослідники визначають як першу війну «в прямому ефірі». Особливість цієї інформаційної війни розкривається в тому, що в ній одразу беруть участь представники багатьох країн, які з однієї сторони: Україна, США, Велика Британія, ЄС, НАТО та інші європейські країни, а з іншої сторони росія та опосередковано Білорусь. Китай в свою чергу займає «*вичікувальну*» позицію, тобто намагається зайняти нейтральну позицію, щоб зрозуміти, до яких наслідків призведе війна в Україні.

Головною проблематикою в контексті цього дослідження є «*інформаційна війна*», функціонування та її особливості, використання різних стратегій інформаційної війни кожної держави разом із веденням військових дій, а також, як вони впливають на політичні процеси в Україні. Тобто, актуальність цієї роботи розкривається через дослідження особливостей перебігу першої війни «в прямому

ефірі» та використання її інструментів та технологій для оцінки специфіки деструктивного впливу на політичні процеси, які відбуваються в Україні та світі як результат російсько- української війни.

Мета кваліфікаційної (бакалаврської) роботи є визначити технології інформаційної війни та дослідити їх специфіку на прикладі російсько-української війни та інших війн, які знайшли свою реалізацію, зокрема на медійному плацдармі.

Ця кваліфікаційна (бакалаврська) робота включає наступні завдання:

(I) визначити сутність поняття «інформаційна війна» та її основні моделі організації;

(II) дослідити інструменти інформаційної війни та особливості їх реалізації;

(III) проаналізувати засоби та методи інформаційних війн в світі;

(IV) визначити сутність поняття «пропаганда» та її заходи й механізми як прояв інформаційної війни;

(V) охарактеризувати та дослідити пропаганду як позитивне явище в контексті формування стратегій державної інформаційної політики;

(VI) ідентифікувати сучасні загрози інформаційній безпеці України під час російсько-українській війні (2014-2024 рр.);

(VII) визначити місце та вплив інформаційної війни в російсько-українській війні (2014-2024 рр.);

(VIII) сформувати перелік засобів й механізмів протидії інформаційній війні для забезпечення інформаційної безпеки в Україні.

Об'єкт дослідження є технології, види, засоби, інструменти та методи інформаційної війн у світі та першої війни в прямому ефірі.

Предметом дослідження є особливості технологій інформаційної війни, які впливають на сучасні політичні процеси в Україні та в світі.

До *методів дослідження* відносяться загальнонаукові та спеціально-наукові методи, що складають наукову основу цієї роботи, зокрема під час написання

кваліфікаційної (бакалаврської) роботи були використані: формально-логічний метод, порівняльний, логічний, діалектичний метод, що дозволили розкрити сутність поняття «інформаційна війна» та «інформаційна війна в прямому ефірі», охарактеризувати інструменти інформаційної війни та особливості її реалізації, що становлять об’єкт дослідження. Також, були використані такі методи як аналіз, синтез системний (структурний і функціональний) метод, які допомогти охарактеризувати розрізі паралелей між сучасним протистоянням в Україні та іншими війнами, зрозуміти технології, які використовувалися в попередніх війнах та сьогоднішній війні. Більше того, загальнонаукові та спеціально-наукові та інші методи допомогли сформувати перелік засобів й механізмів протидії інформаційній війні для забезпечення інформаційної безпеки в Україні.

Аналіз останніх досліджень і публікацій. Дослідження базується на підходах та визначеннях таких українських вчених як: Демедюк, С.В., Магда Є.В., Марков, В.В., Еляшевська, Н., Лубкович, І.М., Почепцов Г.Г. та зарубіжних вчених, зокрема: Г.Г. Саммерса, Г.Е. Екклза, Ден Кюль, Маргарет Роуз, Ч. Пірс та інших досліджень міжнародних організацій Європейського Союзу, аналітичних статтях, тощо.

Структуру роботи. Кваліфікаційна робота складається із вступу, трьох розділів, висновків, списку використаних джерел, що налічує 30 найменувань. Основний зміст викладено на 50 сторінках.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ

1.1. Сутність поняття «інформаційна війна» та основні моделі організації інформаційної війни.

Поняття *«інформаційна війна»* має більш публіцистичний характер, що знаходиться на етапі формування та офіційного визначення. Ден Кюль [Dan Kuehl] з Національного університету оборони визначив поняття *«інформаційна війна»* як *«конфлікт або боротьбу між двома або більше групами в інформаційному середовищі»* [1]. Це визначення можна оцінити як спосіб описати «кібератаку», однак наслідки конфлікту між двома або більше групами, може призвести до масштабніших наслідків ніж втручання або знищення однієї чи більше налагодженої інформаційної системи. Західні лідери інвестують мільярди в розвиток можливостей, створюючи військові командування для атаки, захисту і використання вразливостей електронних комунікаційних мереж. Інформаційна війна об'єднує радіоелектронну боротьбу, кібервійну та інформаційно-психологічні спеціальні операції (ІПСО) в єдину бойову організацію, що слугуватиме як центральний елемент в усіх бойових діях у майбутньому.

Вільний обмін інформацією всередині країни та між державами має важливе значення для бізнесу, міжнародних відносин і соціальної згуртованості, так само інформація необхідна для здатності збройних сил вести безпосередні бойові дії. Зв'язок сьогодні значною мірою спирається на інтернет або через зв'язок з використанням різних частин електромагнітного спектра (таких як радіо або мікрохвилі) через наземні мережі зв'язку або супутникові мережі в космосі.

Інформаційну війну також визначають як форму протистояння або протиборства між державами або неурядовими, політичними, економічними або іншими структурами, що реалізується за допомогою системи заходів й інструментів з

метою завдати шкоди інформаційній сфері опонента та забезпечити захист власної інформаційної безпеки [2].

Перша згадка та визначення «інформаційна війна» (information warfare) з'явилося в середині 1980 років після завершення холодної війни між СРСР з однієї сторони та Західної Європи та США з іншої сторони, що зумовило виникнення нових завдань перед Збройними силами США. Зокрема, такі американські військові теоретики досліджували питання інформаційної війни: Г. Г. Саммерса (1932–1999), Г.Е. Екклза (1898–1986) та інші. Поняття «*інформаційна війна*» почали активно використовуватися в засобах масової інформації після операції *«Буря в пустелі*», яка відбулася в 1991 році й під час якої вперше використовувалися інформаційні технології як інструмент ведення військових дій. Офіційно поняття *«інформаційна війна»* вперше зафіксовано в директиві міністра оборони США від 21 грудня 1992 року №3600 [3].

Доктрина боротьби системи управління, яка була введена в дію в лютому 1996 року міністерством оборони США, визначала поряд з принципами боротьби застосування інструментів інформаційної війни у військові сфері. Згодом у жовтні 1998 року міністерство оборони США ввело в дію «*Об'єднану доктрину інформаційних операцій»*, де згадувалося поняття *«інформаційна війна»* та *«інформаційна операція*» [2].

Якщо визначати інформаційну війну між державами, то пріоритетним завданням буде реалізація прямого негативного та руйнівного впливу на політичну систему держави шляхом ослаблення її функцій та потенційних можливостей, метою яких є забезпечити національну безпеку держави та її громадян. Крім того інформаційна війна може бути направлена на створення перепон та труднощів у внутрішньому розвитку та формуванні зовнішньої політики, а також завданню шкоди політичному іміджу правлячої системи шляхом усунення політичного управління від влади або ослаблення впливу правлячої еліти.

Залежно від сфер функціонування інформації вчені по-різному визначають сутність поняття «*інформаційна війна*». Так, наприклад, у випадку трактуванні інформаційної війни у гуманітарному сенсі, різні види активних методів трансформації інформаційного простору можуть визначатися як інформаційна війна. Зокрема, інформаційна війна реалізується шляхом нав'язування потрібної моделі світогляду, яка прагне забезпечити певні типи мислення.

В свою чергу британські вчені визначають інформаційну війну як вплив на інформаційні системи протилежної сторони з одночасним захистом власних систем. Крім того, словник технологій (TechDictionary) містить наступне визначення, яке було надане Маргарет Роуз (Margaret Rouse), технологічним експертом, «*інформаційна війна – це тактичне і стратегічне використання інформації для отримання переваги, що включає в себе кілька видів операцій і в різні епохи проводилася кардинально різними способами*» [4].

Дж. Стейна і Р. Шафранськи. Дж. Стейн у своїй науковій статті 1995 року «*Інформаційна війна*» говорить про інформаційну війну як про технологію досягнення національних цілей за допомогою інформації [5]. У 1994 році Р. Шафранськи зауважує необхідність та важливість врахування в процесі інформаційної війни ментального виміру й цінностей населення. Предметом інформаційної війни вчений розглядає примус опонента підкоритися волі іншої сторони. Враховуючи вищевикладене, вчений зробив наступний висновок «*Знання цінностей супротивника і використання його репрезентативної системи дає нам змогу співвідносити цінності, спілкуватися з противником на вербальному й невербальному рівнях мовою ворога*» [5].

У науковій доктрині вчені також визначають наступні моделі організації інформаційної війни:

Модель масової демонстрації, яка базується на організації заворушень, протестів та демонстрацій громадянами з певних підстав та причин, яка згодом може

перерости в безсилля влади. Безсилля влади та неможливість врегулювати конфлікт може бути основою для повалення (усунення) існуючої влади іншою політичною елітою, яка є зацікавлена в зміні влади.

Наступною моделлю організації інформаційної війни слід розглянути *модель пропагандистської комунікації*. Як зазначав вчений Л. Войтасий, ця модель пройшла еволюцію в три кроки: а) зміна та переорієнтація громадської думки шляхом введення нових цінностей; б) економічна дезінформація; в) поширення певних моделей кращого життя шляхом використання інструментів засобів масової інформації, розважального контенту тощо [6]. Відповідні кроки сприяють формуванню необхідної картини для людей очікуваного життя/подій, хоча часто очікування й отримана картина не збігаються з дійсністю, тобто у людей створюється відповідна ілюзія, яке не відповідає дійсним реаліям. Наприклад, російська пропаганда ще задовго до початку повномасштабного вторгнення в Україну транслювала на всіх своїх національних каналах, що Україна становить загрозу для росії та планує напасти на росію.

Таким чином, росія довгі роки шляхом пропагандистської комунікації, яка безпосередньо була направлена на громадян росії, сприяла формуванню думки в громадян росії, що Україна становить небезпеку й існує єдиний спосіб усунення цієї небезпеки є проведення так званої «спеціальної операції», що сталося 24 лютого 2022 року.

Однією з моделей організації інформаційної війни є *модель дезінформаційної,* що здійснюється, як правило, масовим впливом на свідомість людей наступним чином: а) привернення та залучення уваги; б) емоційна стимуляція; в) демонстрація як ситуація може бути вирішена та до чого призвести відповідно до висновків комунікатора. Ця модель реалізується шляхом поширення неправдивої інформації, чуток, що мають на меті дезінформувати та заплутати людей, нав’язати певні сценарії розвитку подій.

Модель нейтралізації, яка знаходить свій прояв: а) замовчуванні конфлікту; б) введенні нової резонансної події, яка буде відвертати увагу від важливої іншої події; в) неправдиві спростування або підтвердження інформації, яка буде сприяти досягнення поставленої мети. Мета цієї моделі полягає змістити або навпаки направити фокус уваги громадськості на «*потрібну*» інформацію або проблему. Під час використання цієї моделі інформація важко піддається перевірці, тому громадськість часто сприймає її як достовірну.

Стандартна *модель масової комунікації*, яка включає в себе такі елементи: джерело – кодування – повідомлення – декодування – отримувач. За допомогою цієї моделі може здійснюватися управлінський вплив на свідомість громадськості та нав'язувати свої інтереси різним суб'єктам в інформаційному середовищі [6]. Відповідні комунікації мають не лише інформаційний характер, а наділені політичною значимістю, що відображає конкретні інтереси відповідної сторони, яка веде інформаційну війну.

Ч. Пірс визначає також *семіотичну модель* організації інформаційної війни. Так, існує три типи семіотики, які виокремлюють певні типології визначальних знаків для кожної стадії: а) знаки-індекси, які вказують на іншу інформацію; б) іконічні знаки у вигляді телевізійних знаків (наприклад, кіно ілюструє картину життя, яка не відповідає реальності); в) знаки-символи, які використовує медіа для введення нових пріоритетів для громадськості. При застосуванні цієї моделі населення повинно переорієнтуватися на нав'язані ідеї тільки вербальним способом.

Також слід розглянути *модель резонансного впливу*, особливість якої розкривається в тому, що основою впливу є не новизна інформації, а базування на вже існуючій інформації. Технологія резонансу базується на таких схемах: а) когнітивні схеми; б) комунікативні схеми; в) власне резонансні схеми. У цій технології важливі обидві позиції як слухача так і мовця. Таким чином, аудиторія, що слухає інформацію,

знаходиться на тій самій позиції за важливістю, як і ті, хто розповідає відповідну інформацію.

Таким чином, хоча загальновизнано, що інформаційна війна стала обов'язковим важливим компонентом будь-якого сучасного конфлікту, все ще не існує єдиного загальноприйнятого розуміння того, що саме являє собою інформаційна війна. Однак, все ж таки, проаналізувавши ряд визначень понять, можемо зазначити, що *«інформаційна війна»* – це боротьба між декількома суб'єктами, що здійснюється шляхом використання, руйнування, розповсюдження інформації задля досягнення конкретних цілей супротивника.

Основними моделями організації інформаційної війни є модель масової комунікації, модель нейтралізації, модель пропагандистської комунікації, модель резонансного впливу, семіотичну модель, модель дезінформації та модель масової демонстрації організації інформаційного впливу. Інформаційна війна безперервно здійснюється росією проти України з метою усунення української влади та приведення до влади «проросійських» політиків, що виступатимуть «маріонетковим корпусом управління» та контролюватися політичним управлінням російської федерації.

1.2. Інструменти інформаційної війни та особливості їх реалізації.

Одним із перших проявів інформаційної війни ще до періоду закінчення холодної війни, можна розглядати випадки в індустріальну епоху, коли літаки покривали села чи міста листівками або матеріалами в рамках реалізації зовнішньої політики. У міру того, як індустріальна епоха перейшла в епоху радіо і телебачення, цей тип засобів масової інформації використовувався в інформаційній війні. Під час холодної війни радянські «*активні інструменти*» включали маніпулювання засобами

масової інформації – наприклад, шляхом втручання у створення легітимного документального фільму в Західній Німеччині з метою загострення напруженості через нацистське минуле країни.

Сьогодні майже всі відповідні прояви інформаційної війни пов'язані з цифровими медіа. Прикладами сучасної інформаційної війни є наступальні стратегії вторгнення або руйнування ІТ-інфраструктури противника, а також зусилля щодо захисту ІТ-систем від кібератак. Тобто, сучасна версія інформаційної війни здійснюється через інтернет, що дозволяє охопити широке коло людей.

Наступ росії на Україну назвали першою у світі війною в TikTok, тому що так багато повідомлень як за, так і проти неї зводиться до коротких відео в додатку [7]. Одним із проявів нових інструментів можна визначити створення ботів у Twitter (нині X), які зазвичай використовуються для поширення важливої інформації широкому колу людей щодо прикладу обов’язковості вакцини проти COVID-19, були перетворені на вужчу спробу підтримати російське вторгнення. Компанії з великою онлайн-аудиторією намагалися обмежити поширення проросійських повідомлень, але їхні постачальники знаходили способи обійти це.

Twitter вперше почав публікувати дані, пов'язані з «інформаційними операціями, підтримуваними певною державою» на своєму сервісі майже п'ять років тому. Через кілька років після цього він детально описав пов'язані з цим правоохоронні зусилля, такі як видалення сотень венесуельських облікових записів, які повторювали офіційні урядові наративи, та інші нападки на лівійський уряд. Невдовзі після вторгнення в Україну Twitter почав позначати певні твіти, що містять посилання на російські державні ЗМІ, а також заклик «бути в курсі подій» [7]. У росії уряд просто заблокував Twitter та інші соціальні мережі, щоб обмежити доступ своїх громадян до інформації про війну в Україні та її реальні цілі, мету, втрати та інше.

Сучасна інформаційна війна використовує систему інструментів, які постійно оновлюються та прогресують з метою завдати негативних наслідків противнику. До

таких інструментів ми можемо віднести: *радіоелектронну боротьбу, кібератаки, інформаційно-психологічні операції (ІПСО)*, що створюють систему інструментів, які використовуються під час інформаційної війни.

Радіоелектронна боротьба як один із видів інструментів інформаційної війни використовується для порушення або нейтралізації електромагнітних передач, які, серед іншого, забезпечують обмін інформації. Це можуть бути електронні засоби протидії та глушіння, які використовуються для виведення з ладу систем військового зв'язку або наведення зброї. Також це може включати цивільне використання, наприклад, систему управління повітряним рухом ADS-B, яка використовується повітряними суднами для уникнення зіткнень під час польоту, або прийняту Європейську систему управління залізничним рухом (ERTMS), яка замінює залізничний колійний сигнал та забезпечує повний контроль над поїздами. Глушіння або погіршення будь-якого з них призведе до порушення роботи транспорту (повітряного або надземного).

Наступним інструментом інформаційної війни можна розглядати *кібератаки*, що здійснюються через інтернет проти цифрових мереж, які можуть унеможливити роботу бізнесу або навіть призвести до порушення роботи такої складної системи як держава, наприклад як зазіхання на роботу державних банків або операторів зв’язку. Ці атаки можуть спричинити величезні збитки, як за вартістю, так і по репутації, політичного іміджу управлінської еліти, наприклад, як видно з атак на Sony Pictures і TalkTalk, якщо ми говоримо про європейський ринок, або ж нещодавні атаки на одного із основних операторів зв’язку в Україні «Київстар» або ж атаки на ПриватБанк та Монобанк, які здійснюються росією проти України під час введенні росією гібридної війни проти України. Кібератаки також можуть бути спрямовані на промислові системи управління, що використовуються на виробничих підприємствах або в енергетичних, водо- та газових компаніях. Маючи можливість впливати на такий

широкий спектр національної інфраструктури, життя людей може бути поставлено під загрозу.

Інформаційна війна може застосовувати також такі інструменти як *інформаційно-психологічні спеціальні операції (ІПСО)*, які більше спрямовані на погіршення морального та психологічного стану громадян країни. Це може включати поширення неправдивої інформації, чуток і страху через соціальні мережі та новинні агентства. Високий рівень зв'язку, який сьогодні мають люди у всьому світі, є сильною стороною, але миттєвий зв'язок означає, що дезінформація та страх також можуть швидко поширюватися, що призводить до паніки та хаосу всередині організації та/або держави.

Отже, можемо визначити інформаційну війну як інтеграцію таких видів боротьби як радіоелектронна боротьба, кібервійни та інформаційно-психологічні операції як для здійснення збройного нападу, так і для оборони. Російська федерація постійно здійснює інформаційні атаки на сусідні держави, зокрема проти України, Грузії, Естонії, Польщі, Литва та Латвії, які постійно зазнають комплексного натиску електронних, кібератак та інформаційно-психологічних операцій. Прикладом, що росія веде війну гібридну війну, що включає в себе інформаційну війну, не тільки проти України, але й проти інших держав, є переконливі непрямі докази того, що газопровід Баку-Тбілісі-Джейхан у Грузії був атакований за допомогою складного комп'ютерного вірусу, який спричинив неконтрольоване підвищення тиску, що призвело до вибуху.

2. ФОРМУВАННЯ ТА ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ ІНФОРМАЦІЙНОЇ ВІЙНИ

2.1 Засоби та методи інформаційних війн у світі.

Зазвичай інформаційна війна не є окремою технікою ведення війни. Інформаційна війна може поєднувати в собі різні форми, щоб створити більшу та сильнішу концепцію протистояння. Мартін Лібіцкі визначив сім форм інформаційної війни, а саме: (I) командно-контрольна війна, (II) інтелектуальна війна, (III) електронна боротьба, (IV) психологічна війна, (V) економічна інформаційна війна, (VI) хакерська війна; (VII) кібервійна [8].

Командування та контроль в організації армії, обізнаність про ситуацію є надважливим аспектом для командирів, щоб приймати правильні рішення в критичних ситуаціях. Нездатність отримати точну та своєчасну інформація із землі перешкоджатиме процесу прийняття рішень командирів. Отже, питання командирів і зв'язку відіграє першочергову ролі у введенні, зокрема інформаційної війни. Точна поінформованість та вміння приймати рішення повинні існувати для ефективного функціонування війська. Для досягнення мети військової операції лідера противника потрібно дезорієнтувати шляхом поширення неправдивої інформацією, інформаційні лінії передачі повинні бути скомпрометовані або знищені. У той же самий час, під час інформаційної війни потрібно налагодити захист та безпеку поширення інформації всередині країни, війська, та організувати належний рівень захисту так званих ліній передач інформації.

Інтелектуальна війна – це не тільки інтелектуальне збирання інформації, але й інтелектуальна отримання інформації з пристроїв або датчиків, які подаються безпосередньо в операційну систему противника. Супутникові знімки, що відображають рух військ противника, яке у подальшому допомагало б визначити

власний курс дій та заходів. Інтелектуальна система озброєння сприяє зменшенню навантаження на бойові війська. Відповідні системи дозволяють вистрілювати із них, а відповідні датчики, які встановлені у системі озброєння прокладають та формують шлях до заздалегідь визначених цілей. Якщо датчики або ж інформацію (сигнал), які передають датчики, може бути скомпрометована, постріл може навіть повернутися назад до місця вистрілу.

Електронна боротьба має довгу історію війни. Вона стосується, зокрема електромагнітного випромінювання, основною метою якого є погіршення фізичної основи для перенесення інформації. Електронні боротьба може використовуватися для пошуку ідентичності та місцезнаходження джерел випромінювання електромагнітної енергії для нападу на людей, об'єкти чи обладнання та для захищення власного війська, приміщення та техніки від будь-якого впливу електронної боротьби.

Психологічна війна передбачає використання інформації проти людського розуму. Телебачення, радіо та інтернет відіграють дуже важливу роль у психологічній війні. Загальне населення Сполучених Штатів можливо б не підтримувало напади на Ірак та Афганістан, якщо б постійно не здійснювалося транслювання наскільки лідери цих держав є погані та небезпечні для миру в світі. Побачене часто означає те, чому можна вірити, (наприклад, Сполучені Штати Америки через свій один із найвідоміших телеканалів (CNN) транслює необхідну інформацію для суспільства Америки і не тільки). Реформаційний рух в одному з південних регіонів Азії є прикладом психологічної війни проти супротивника командирів або лідерів. Лідери правлячих партій охарактеризовані як такі, що пов'язані всіма видами корупції, зловживання владою, практики кумівства тощо. Правлячі партії використовують телебачення, газети та радіо для протидії нападу зі сторони опозицій і водночас створюють страх у більшості суспільства переходу влади та контролю опозиції. У

психологічній війні правда є неважливою, доки мета або бажання лідерів країн досягаються.

Економічна інформаційна війна складається з інформаційної блокади та інформації імперіалізму. Інформаційна блокада працює, змушуючи цільову країну працювати у темряві та в довгостроковій перспективі, позбавляючи переваги обміну інформацією. Наслідки можуть бути катастрофічними для країн, які так сильно залежать від інформації. Відрізання їхніх ліній зв'язку призвело б до зупинення їх бізнесу. Інформаційний імперіалізм – це система та методи ідеологічного впливу монополізованих засобів масової інформації великих капіталістичних держав на інші країни. Країни борються одна з одною за домінування в стратегічній економіці промисловості, зокрема торгівлі. Деякі галузі кращі за інші. Контроль над нафтою в Близькому Сході може бути однією з причин нестабільності регіону протягом такого тривалого часу.

Хакерська війна значно відрізняється. Це може бути зроблено окремою особою або групою осіб, які об’єднані спільною метою. Це вже не новина чути про веб-сайти перестають працювати, дані кредитної картки викрадаються через інтернет. Це відбувається під час війни в Перській затоці, де військові об'єкти Сполучених Штатів Америки було зламано з метою викрадення інформації та у подальшому фактично запропонована Саддаму Хусейну, іракському державному службовцю [9].

До основних принципів інформаційної війни, які визначав, зокрема, Даніель Е. Магсіг можна віднести: (I) відмова, (II) посилення сили, (III) виживання, (IV) ситуаційна обізнаність, командування, контроль; (V) комунікації та їх рівень [10].

Інформація про силу і слабкість ворога, власну і дружню сили важливі для перемоги у війні. Відмова від цієї інформації тримало б у невіддані командирів війська, що б призвело до втрати контролю та ситуації над військом. У зв’язку з цим центри управління, системи підтримки прийняття рішень і зв'язку є основними цілями для знищення під час введення будь-якої війни.

Наступний принцип – це **посилення сили**, що реалізується наступним чином. Війська на землі потребують інформації так само, як і їхні командири. Потік інформації зверху вниз має бути якомога більш гладким, щоб зменшити або уникнути додаткового ризику та конфлікту всередині війська.

Децентралізація важлива для забезпечення виживання. Політика і стратегія будь-якої війни має бути централізовано на верхньому рівні, але також надання певного рівня свободи дій нижчому рівню (виконавцям), щоб вони могли планувати та виконувати свої місії. Сумісність є іншим аспектом, який необхідно забезпечити для того, щоб вижити. Вся інформаційна та комунікаційна система повинна мати можливість спілкуватися один з одним, щоб забезпечити максимальний обмін інформацією.

Останній принцип інформаційної війни – це **рівень,** який стверджує, що всі доступні технології слід використовувати проти ворожих сил, які не мають істотного значення для можливостей ворога. Інтенсивність конфліктів інформаційної війни має бути направлена на вичерпування зусиль противника в інформаційній війні.

Крім того, Reto E. Haeni перерахував кілька прикладів можливих заходів, які можуть використовуватися військовими та терористами наступним чином:

(I) *Комп'ютерні віруси* – це фрагмент коду, який копіюється у більшу програму для зміни цієї програми. Вірус запускається лише тоді, коли його хост-програма починає бігати. Потім вірус розмножується, заражаючи інші програми коли він розмножується [10];

(II) *Хробак* – це незалежна програма, яка розмножується шляхом копіювання самого себе, а саме: повномасштабний код з одного комп’ютера на інший, зазвичай через мережі. На відміну від вірусу, він зазвичай не змінює інші програми [10].

(III) *Троянський кінь* – це фрагмент коду, який ховається всередині програми виконує приховану функцію. Це популярний механізм маскування вірусів чи хробаків».

(IV) *Логічні бомби* – це тип троянського коня, який використовується для випуску вірусу, хробака або якась інша системна атака. Це або незалежна програма, або частина коду, яку вставив розробник системи або програміст». [10]

(V) *Люк, або задні двері* – це механізм, вбудований у систему його дизайнером. Функція люка полягає в тому, щоб надати дизайнеру спосіб проникнути назад у систему, обходячи звичайну систему захисту.

(VI) *Сколювання,* що дозволяє виробнику легко налаштувати чіпи так, щоб вони містили деякі несподівані функції. Їх можна побудувати так, щоб вони потім зазнали краху в певний час, підірвати після отримання сигналу на певний частоті або надсилання радіосигналів, які дозволяють ідентифікувати їх точне місцезнаходження.

(VII) *Наномашини та мікроби* дають можливість викликати серйозні пошкодження в системі. Вони можуть бути використані для атаки на апаратне забезпечення в комп'ютерній системі.

(VIII) *Електронне глушіння* використовується для блокування каналів зв'язку противника обладнання, щоб вони не могли отримати жодної інформації.

(IX) *Гармати HERF* – Бомби EMP. HERF означає High Energy Radio Frequency. Гармати HERF здатні стріляти потужним радіосигналом по електронній цілі та гасити її функції. Ураження може бути середнього або важкого ступеня. По суті, гармати HERF – це так звані радіопередавачі, які посилають концентрований радіосигнал до цілі.

EMP означає електромагнітний імпульс. Джерело може бути ядерним або неядерної детонації. Це руйнує електроніку всього комп'ютера й системи зв'язку на досить великій території. ЕМП бомба може бути меншим, ніж гармата HERF, щоб викликати подібну кількість шкоди і зазвичай використовується для ураження не однієї цілі, а всіх обладнань, що знаходиться біля бомби.

(X) *Випромінювання Ван Ека* – це випромінювання, яке здійснюють всі електронні пристрої. Спеціалізовані приймачі можуть вловити відповідне

випромінювання та отримати велику кількість інформації. Наразі існують різні засоби захисту від цього типу атак.

(XI) *Криптологія* – це зброя інформаційної війни, яка призначена для шифрування й злами безпечних комунікаційних зв'язків. Незважаючи на значні прогрес у криптографії, криптоаналіз є надалі важливою зброєю, якому сприяють не менш значні досягнення в обчислювальній потужності техніці.

(XII) *Відео Морфінг* – це так зване перетворення відео, що використовується як зброя, яку можна використати для створення іншого бажаного результату, наприклад, що ворожий лідер говорить те, чого він або вона насправді не говорив з метою підірвати довіру суспільства.

2.2. Сутність «пропаганди» та її засоби і механізми як прояв інформаційної війни.

Негативне сприйняття терміну «пропаганда» зводилося до вивчення того, що пропонується як його класичний приклад – праці ідеологів фашистської Німеччини. Однак, саме явище і термін *«пропаганда»* зазнали серйозних змін
за тривалий історичний період їх існування.

Спочатку цей термін використовувався для позначення місіонерської установи, яка була заснована в Римі в 17 столітті та мала на меті поширення католицизму серед язичників. Однак у роки французької революції, термін набув політичного відтінку і став асоціюватися з діяльністю в таємних товариствах, які прагнули поширювати ідеї в інших країнах через своїх емісарів (представники державної служби та/або спеціальних служб). Безсумнівно, з моменту зародження пропагандистських прийомів і методів обміну масової інформації багато чого розвинулося та вдосконалилося, а сама пропаганда стала потужним інструмент мобілізації.

Сучасна наука пропонує досить широкий спектр визначень пропаганди. Професор І.Б. Орлов виділяє три основні з них: (I) перше визначення ґрунтується на тому, що висновки або узагальнення робляться на підставі сумнівних або односторонніх аргументів, і деяких аргументів або замовчуються, або відверто дискредитуються. (II) Під другим визначенням розглядається як спосіб поширення хибних ідей. (III) Третє визначення включає в себе сферу пропаганди, а саме: широка сфера соціальних відносин, включаючи філософію, освіту, політику, журналістику, мистецтво» [11]. Тобто, слід погодитися, що пропаганда є широкою категорію, що може охоплювати найрізноманітніші сфери діяльності.

Альтернативні визначення цього явища припускають, що погляди, ідеї держави, сформовані пропагандою, впливають на поведінку людей. Проте з часом пропаганду вчені почали визначати вужче як діяльність, спрямовану на поширення ідеології та політики конкретних класів, партій і станів у масах. Така перспектива підкреслювала характер пропаганди і зазначала, що в суспільній думці поняття пропаганди часто використовується як синонім брехні та засобу маніпулювання свідомістю. Ця інтерпретація була зумовлена навмисним бажанням зобразити пропаганду як «універсальне зло сучасної цивілізації». Можна спостерігати, що радянська пропаганда отримала подібні, дзеркальні оцінки на Заході. Протягом XX-го століття *«пропаганда»* використовувалася в різних сферах як засіб політичної дискредитації опонентів.

У радянський період розвитку сучасні вчені-ідеологи намагалися продемонструвати непослідовність і неефективність комуністичного (більшовицької) пропаганди. Однак, результати громадянської війни в Росії, Другої світової війни та період масового будівництва та освоєння *«нових земель»* виявили, що повідомлення правди і надія на перемогу, і благополучне майбутнє мала могутній мобілізуючий вплив на радянських людей. Зокрема, багато питань постало тоді, коли політичні орієнтації стали неясними, партійна та радянська бюрократія розширилася, виникла

розбіжність між словами і діями (подвійні стандарти), спричинивши втрату сили та дієвий зміст пропаганди.

Комуністична партія не змогла дати відповіді на гострі життєві питання. Пропаганда переросла в порожні дифірамби, такі як «*Наздогнати і перегнати*» (Америку), «*Партія і народ єдині*», «*Економіка має бути економною*», «*Вперед, до нових перемог комунізму*». За цими словами не було ніякого змісту. Ідеологічні посили не відповідали реаліям часу [12].

Пропаганда, що пропагує переваги радянського способу життя, з його скромним побутом і процвітання, не змогла протистояти привабливості глянцевого західного суспільства масового споживання. Більше того, ранні методи пропаганди втратили свою ефективність, оскільки вони не справлялися з проблемою потреб нової, більш освіченої та грамотної аудиторії. Коли залізна завіса впала, з'явилась інша картина – західне життя, яке, хоча й не було таким ідеальним, як вважалося спочатку, було далеким від того нещасного, злиденного й розчавленого образу капіталізму, намальованого радянською пропагандою. Отже, радянська пропаганда зазнала нищівної поразки після холодної війни.

Ідеологічне протистояння продемонструвало, що якість і ефективність пропаганди залежить від багатьох факторів. До числа найважливіших відносяться сумісність ідей, цінностей та перспектив, які закладаються в основу пропаганди, з потребами та вимогами соціального розвитку та аудиторії, а також сумісність ціннісних суджень пропагандистського дискурсу з реаліями життя. Радянська пропаганда не змогла довести перевагу свого ладу та способу життя, а не обманювати, спотворювати та поширювати ідеї, погляди та цінності, не навязуючи їх іншим. Проте варто зазначити, що на фінальній стадії протистояння між двома системами, виникла теорія контрпропаганди. Цей розвиток подій свідчить про те, що звернення до контрпропаганди могло актуалізуватися необхідність так званої «*сірої*» та *«чорної»* пропаганди.

Різні ступені використання ЗМІ як зброї, способи її застосування, й об’єкти орієнтації проявляються в різних видах протистояння, як зафіксовано в таких поняттях, як *«ідеологічна війна», «холодна війна», «психологічна війна»* та *«морально-психологічна війна»*, «*інформаційна війна*». Всі ці поняття відображають різні аспекти і нюанси одного і того ж явища, що охоплює історичні, соціально-політичні особливості протистояння та унікальне соціально-психологічне сприйняття впливу на реального чи потенційного ворога. Зміст справи розкривається в тому, що інформація служить основою впливу в усіх цих видах протистояння.

Переходячи до розгляду взаємозв’язку між пропагандою та інформаційною війною, потрібно відзначити, що в більшості робіт дослідники зосереджуються на їх загальних характеристиках, нехтуючи специфічними особливостями. Наприклад, зарубіжні дослідники, досліджуючи зв'язок між поняттями «*антидержавна пропаганда*» та «*інформаційна війна*», розпочинаючи їх аналіз з дуже простого співвідношенням: «*Ведення інформаційної війни виражається в ідеологічній пропаганді власних політико-ідеологічних установках з використанням широкого спектру засобів*».

Таким чином, автори вважають доцільним зробити висновок про те, що еквівалентність понять *«інформаційний вплив на масову свідомість як частина інформаційної війни»* та *«антидержавна пропаганда»* пропонують використовувати їх як синоніми.

Важливо зазначити, що розгляд процесу пропаганди та її вплив необхідно включати в широкий ідеологічний, соціально-психологічний і владний контексти, але також виходять з того, що пропаганда — це *«взаємопов'язана система методів і технології, метою яких є інтеграція особистості в суспільство та ізоляція від неї альтернативних інформаційних потоків (що знижує протестні настрої) і запропонувати їм просту орієнтацію схеми відповіді на життєво важливі питання»* [13].

Водночас фактична реальність показує, з одного боку, вкрай негативне ставлення до пропаганди, а з іншого – звернення фахівців-дослідників до нового явища – інформаційної війни і, як наслідок, повне забуття пропаганди або її «прокляття». Дійсно, пропаганда була витіснена з наукового поля академічних досліджень. Тим часом американські вчені посилаються на нову концепцію ноополітики (Arquilla and Ronfeldt, 1999), в якому пропаганда, на їхню думку, має зайняти належне їй місце.

Виявлення сутнісних характеристик інформаційної війни потребує визначення її подібності та відмінності від пропаганди та контрпропаганди, хоча на практиці, вони тісно переплетені між собою і їх важко розрізнити. Пропаганду для іноземних держав часто використовують як інструмент війни – хитру суміш чуток і обман, правда є лише приманкою для підриву єдності та сіяння плутанин. По суті, пропаганда є вершиною первісного проникнення, підготовки населення на території, яка обрана для вторгнення. Це перший крок, потім вступає в дію п'ята колона за ними йдуть диверсійно-десантні підрозділи, або «*командос*», і дивізії вторгнення» [14].

Пропаганда трактується як поширення певних поглядів і знань в суспільстві за допомогою їх постійного детального пояснення і як система заходів, спрямованих на поширення знань, художніх цінностей та іншої інформації для формування певних поглядів, ідей, та емоційних станів, що впливають на соціальну поведінку людей, а також як популяризація політичних, філософських, релігійних, наукових, мистецьких та інших ідей в суспільстві через розмовну мову, ЗМІ, візуальні та інші засоби впливу на суспільну свідомість.

Крім того, під пропагандою розуміють послідовну, достатньо тривалу діяльність, спрямовану на створення або інформування різноманітних подій з метою впливу на ставлення мас до питання чи явища; механізм широкомасштабної індоктринації; негативну або оманливу інформацію, яка використовується для підтримки зацікавленість проблемою, яку потрібно вирішувати; навмисно

спровокована та зрежисована кампанія, щоб змусити людей прийняти певну точку зору, позицію чи цінність. «Пропаганда часто асоціюється з *«промивання мізків»* – дезінформація або дії, що заслуговують осуду з точки зору громадськості.

На думку Гарольда Лассвелла, це саме робота держави над формуванням думок громадськості щодо військових цілей на зовнішньому та внутрішньому фронтах є правдивою пропагандою, оскільки для досягнення стратегічних цілей необхідно згуртувати суспільство та мобілізувати його громадян для боротьби з ворогом. Пропаганда поряд з військовою і дискримінаційними економічними заходами, є одним з основних знарядь боротьби з суперниками та противниками.

До того ж, як зазначає американський політолог, сама пропаганда має військове походження: *«Коли суспільство доведене до усвідомлення того, що війну розпочав ворог ... то можна сказати, що пропагандист майже досяг своєї мети ... Кожен народ, який почав війну, обов'язково повинен бути невиправним, корумпованим і розбещеним. Наголошуючи безпосередньо на цих його властивостях, ми лише вживаємо заходів обережності головна мета якого – переконати, що ворог навіть здатний на таке жахливе як наступальна війна. <...> Ворог не тільки зарозумілий, він жадібний. Противник проводить пропаганда, заснована на брехні. Ворог зарозумілий, грубий і жорстокий*» (Лассуел, 1949) [15].

2.3. Пропаганда як позитивне явище в контексті формування стратегій державної інформаційної політики.

Позитивна пропаганда використовується, щоб викликати позитивні емоції в суспільства. Рекламодавці використовують загальні твердження та зображення в позитивному сенсі. Пропаганду також можна використовувати для сприяння єдності, солідарності та злагоди між людьми під час конфліктів. Таким чином, пропаганда

може бути позитивною, якщо вона використовується для допомоги людям і сприяння позитивних змін у суспільстві. Позитивну пропаганду можна використати, щоб збудити сильні почуття патріотизму, а також мобілізувати людей для спільної підтримки доброї справи, такої як падіння апартеїду, який був рішуче підтриманий у всьому світі саме цим методом, також приклад нашої війни та роботи медіа на початку повномасштабної російсько-української війни, що безсумнівно сприяло об'єднання людей для боротьби проти російської агресії та пробудження у громадян України патріотизму.

Позитивну пропаганду можна ототожнити з широко поширеними образами, що зображують позитивні аспекти війни. Вони підтримували військові зусилля, показуючи хоробрих, надійних і скромних солдатів на фронті та мирні та доброчесні родини на батьківщині. Це може стосуватися гендерних прав, громадянських прав тощо. Це відповідає Цілям сталого розвитку ООН щодо миру, справедливості та міцних інституцій.

Зараз у світі триває понад 40 активних конфліктів. Однак не всі війни привертають увагу ЗМІ. Для того, щоб одні війни віддавали перевагу іншим, потрібна сильна присутність пропаганди. Дослідники розглядають наступну гіпотезу про те, що, кожен конфлікт ведеться принаймні на двох підставах: (I) на полі бою та (II) умах людей через пропаганду [16].

Зокрема, хороші хлопці проти поганих хлопців, ми проти них – це ефективні інструменти для забезпечення того, щоб громадськість підтримувала війни, які ведуть уряди. Це явище можна порівняти з конкурсом краси, всі жінки, які беруть участь у ньому, прекрасні, але лише три піднімуться на подіум, а одна стане переможницею. Це стосується війни в Біафрі, яка відбулася в Нігерії в 1960 роках, і війни проти апартеїду в Південній Африці. Обидві війни привернули величезну увагу ЗМІ, і вони також були висвітлені в мистецьких роботах різних митців, таких як Medu Art Ensemble, The Sestigers (Sixtiers) та багатьох інших.

Війна в Біафрі — громадянська війна між урядом Нігерії та Республікою Біафра, сепаратистською державою, яка проголосила свою незалежність від Нігерії в 1967 році. Війну очолив Чуквумека «Емека» Одумегву-Оджукву, який оголосив Біафру незалежною державою і почалася громадянська війна. Він був лідером, який очолював біафрський народ.

Біафрська пропаганда зіграла ключову роль у політичному та дипломатичному веденні громадянської війни в Нігерії. Їхня пропагандистська кампанія зображувала війну як єдину можливу відповідь на кампанію геноциду проти них. Ця війна використовувала різні ЗМІ для поширення своєї пропаганди. Уряд Біафри використав Радіо Біафра як інструмент пропаганди для пропаганди війни як геноциду. Пропаганда Біафри була розроблена, щоб створити цілісне повідомлення та мала на меті викликати співчуття світової громадської думки та прищепити дух виживання серед населення вдома, незважаючи на дуже обмежені комунікаційні ресурси.

Активісти проти апартеїду рішуче виграли цю війну, особливо в міжнародних ЗМІ. Апартеїд був системою інституціоналізованого расового гноблення, яка існувала в Південній Африці з того часу, як європейці вперше окупували Південну Африку в 17 столітті, але була офіційно легалізована в 1948 році. Палестино-ізраїльська війна вперше відбулася в 1947 році, і вона все ще триває, однак апартеїд та інші війни, що відбулися після нього, привернули більше уваги ЗМІ. Це явище несправедливе, але воно все одно приносить користь людям, які постраждали від цих звірств [17].

Кампанії з ліквідації апартеїду були найефективнішою формою привернення уваги ЗМІ. Цю війну, як і багато інших, розпочали, реалізували та підтримали студенти. Цей рух був протестом проти інвестицій американських компаній в південноафриканський уряд апартеїду. Найуспішніша загальнонаціональна кампанія за вилучення відбулася в 1970-х і 1980-х роках, коли студентські організації по всій країні почали протестувати. Студенти були в авангарді кампаній проти апартеїду.

Були й інші політичні протести, що відбулися після руху за відчуження інвестицій, але жоден не був більш помітним, ніж широко висвітлений у ЗМІ студентський протест у Соуето в червні 1976 року. Це повстання було протестом проти уряду апартеїду, який почався в Соуето. Цей протест назавжди залишиться в пам'яті людей завдяки неймовірно ідеальній фотографії, зробленій під час протесту. Як зазначено в статті журналу Time, ця фотографія підштовхнула світ проти апартеїду, автор Арін Бейкер.

Отже, через просування позитивної пропаганди можна досягти миру. Хоча існує тонка межа між індоктринацією та позитивною пропагандою, за цим потрібно уважно стежити. За словами Мартіна Лютера Кінга, вирішальним чинником у тому, чи є пропаганда доброю чи поганою, є достоїнство справи, яку закликають. Позитивна пропаганда є складним поняттям, і її дійсно важко відрізнити від негативної пропаганди.

Однак, важливо, щоб люди, які мають доступ до громадських платформ, використовували свій голос на благо, а позитивна пропаганда є необхідним інструментом, але її слід залишити лише в руках тих, хто хоче сприяти добрій справі, наприклад, забезпечення миру в свої державі, подолання апартеїду.

РОЗДІЛ 3. ВПЛИВ ІНФОРМАЦІЙНОЇ ВІЙНИ НА ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

3.1. Сучасні загрози інформаційній безпеці України під час російсько-українській війні (2014-2024 рр.).

Росія активно застосовує інформаційні операції для підриву України принаймні з 2014 року, про що дослідники Digital Forensic Research Lab (DFRLab) у всьому світі детально задокументували під час своїх постійних моніторингових зусиль. Напередодні вторгнення в лютому 2022 року росія використовувала дезінформацію у формі «*наративної війни*», щоб виправдати військові дії, замаскувати своє планування та заперечити будь-яку відповідальність за війну. Як детально описали дослідники DFRLab у своєму звіті за лютий 2023 року «Підрив України: як Кремль використовує інформаційні операції, щоб підірвати глобальну довіру до України», інформаційна стратегія росії почала змінюватися після вторгнення 2022 року, зосереджуючись на підриві здатності України чинити опір [18].

Повномасштабна війна в Україні триває вже третій рік, росія подвоїла свої зусилля по всьому світу, щоб підірвати міжнародне становище України, намагаючись підірвати підтримку Європи та Сполучених Штатів Америки та внутрішній моральний дух українців. Багаторічне пильне спостереження не лише за державними ЗМІ, такими як Russia Today (RT) та Sputnik, а й за російською активністю в Telegram, TikTok, X та інших соціальних платформах, вказує на один висновок: у пропагандистській війні росія залишається повністю відданою веденню інформаційної війни, зокрема операцій по всьому світу, граючи в довгу гру, щоб перемогти будь-яку єдність між союзниками України та наполягати доти, доки Україна не втратить волю до боротьби.

Західні санкції, запроваджені після початкового вторгнення, порушили здатність росії охопити деяку європейську аудиторію за допомогою своїх державних ЗМІ. Але з тих пір росія скоригувала свої інформаційні операції, щоб більше зосередитися на соціальних мережах. Окрім, напад на підтримку західної громадськості для фінансування оборони України, вона розширила цілеспрямовані пропагандистські зусилля в різних частинах світу, включаючи Латинську Америку, Африка та Близький Схід. Крім того, підтримка України Заходом справді постійно стає предметом дискусій на Заході, особливо у Вашингтоні, де додаткова допомога Україні місяцями затримується в Конгресі. Багато факторів впливають на підтримку виборцями та законодавцями відправки зброї та фінансової допомоги в Україну. Російська пропаганда має на меті призвести до зменшенні західної матеріальної підтримки оборони України, що являє собою чітку мету інформаційної війни президента Володимира Путіна [19].

На другому році війни, зіткнувшись із міжнародними санкціями, зіпсованою репутацією та забороною спонсорованих державою RT і Sputnik у багатьох західних країнах, росія перейшла до більш цілеспрямованих операцій впливу, використовуючи TikTok, Telegram та інші соціальні платформи для розширення своєї міжнародної аудиторії, особливо на Глобальному Півдні, де російські державні ЗМІ все ще є великими гравцями. росія також поглиблює співпрацю у медійній та інформаційній сферах із співчуваючими країнами. Протягом 2023 року росія покладалася на свій багатий арсенал інструментів для проведення інформаційних операцій, включаючи використання скоординованих неавтентичних мереж на платформах соціальних мереж, використання регіональних претензій до Заходу, хакерські атаки та підробку документів, серед інших тактик.

Росія продовжує посилювати контроль над своїм внутрішнім інформаційним простором, поширювати неправдиві та оманливі наративи, щоб послабити рішучість України, і представляє свої поточні аргументи на користь війни через RT і Sputnik,

адаптуючи свої повідомлення до регіональної аудиторії, особливо в Латинській Америці та Африка.

До лютого 2022 року, західний світ визнав, що RT і Sputnik є інструментами російської пропаганди, а не легітимними джерелами інформації. Тим не менш, ці ЗМІ все ще популярні та впливові в деяких частинах Латинської Америки, Близького Сходу та Африці. Більше того, навіть у Європейському Союзі, де ці канали технічно заблоковані, RT обходить обмеження та продовжує отруювати медіапростір через менші дзеркальні сайти, фактично *«обходячи»* західні санкції. Деякі канали показують російський пропагандистський контент, перекладений місцевими мовами. Водночас росія продовжує використовувати свої посольства та дипломатів як продовження свого пропагандистського апарату, просуваючи неправдиву інформацію, неправдиву перевірку фактів та змови по всьому світу [20].

Росія також використовує дипломатичні заходи, такі як саміт Росія-Африка, щоб поширювати свої меседжі на більш регіональному рівні. Російські інформаційні операції та операції впливу в Україні та за кордоном, ймовірно, продовжуватимуть розвиватися, знаходячи нові розбіжності в суспільствах, які потрібно поглиблювати, та нові підходи до їх використання.

Дослідники з Організації Північноатлантичного договору (НАТО) стверджують, що «*російські кібератаки на урядові та військові центри командування та управління, логістику, екстрені служби... повністю відповідали так званій стратегії «громового бігу», спрямованій на те, щоб посіяти хаос, плутанину та невизначеність і, зрештою, уникнути дорогої та затяжної війни в Україні*.» [21].

Другий рік війни росія залишається втягнутою в затяжний конвенційний конфлікт, який, крім запеклих боїв і ракетних ударів, супроводжувався саботажем, насильницьким переміщенням і викраденням дітей, систематичними зґвалтуваннями і тортурами, а також погрозами застосувати ядерну зброю. На думку дослідників НАТО, росія не розпочала тотальну і дорогу кібервійну проти України чи її

прихильників на Заході. Так званий «громовий біг» так і не відбувся. [16]. Скоріше, поєднання української рішучості, характеристик кіберсфери та бажання росії вести глобальну кампанію, зосереджену більше на дезінформації та підриві підтримки Києва.

Однак, окремо потрібно розглянути кібератаки та операцій як все ще існуючу загрозу під час територіального вторгнення збройних сил російської федерації в Україну, що постійно, зокрема, супроводжуються руйнівними кібератаками, і наочно демонструє цю тенденцію до застосування кібератак під час збройних конфліктів у світі. Використання кібератак як засоби ведення війни також спостерігалися раніше між державами, включаючи російську федерацію, Грузію, Ізраїль та Іран, при цьому росія розгортає кібератаки проти України ще з 2014 року. Інститут кібермиру документує кібератаки на критичну інфраструктуру та цивільних об'єктів з початку російської загарбницької війни проти Україна.

Фіксування атак сприяє аналізу використання кіберзасобів у воєнний час. Станом на 31 травня 2023 року Інститут зафіксував 1998 кібератак та операцій, здійснених 98 різними особами. Ці кіберінциденти торкнулися 23 різних секторів критичної інфраструктури, що вплинули на Україну. Під час російсько-української війни, саме застосування звичайних озброєнь в даний час досягає більшого видимого і більш вимірюваного впливу. Проте, як зауважив Крістіан-Марк Ліфландер, керівник відділу нових викликів безпеці Відділу кібер- та гібридної політики (CHP) (ЄСК) в НАТО: «*На відміну від нарощування військ чи інших форм військової мобілізації, які є нечастими та дуже видимими, кібероперації є результатом операційних циклів, які відбуваються приховано і безперервно протягом мирного і воєнного часу. Націлювання на конфіденційні мережі в мирний час дозволяє зловмисникам закласти основу для шкідливого програмного забезпечення, призначеного для використання у воєнний час».*

Кібератаки з руйнівними елементами можуть призводити до перешкоджання доступу до телекомунікацій та інтернет-сервісів, обмежувати доступ до банківських рахунків клієнтів банку, переривання доступу до новин; перешкоджання в доступі до електрики, опалення та води. Наприклад, 28 березня 2022 року кібератака на Укртелеком призвела до обвалу зв'язку до 13% від довоєнного рівня, при цьому спостерігалися загальнонаціональні перебої. Поширення дезінформації та пропаганди, у тому числі через атаки на медіа сектор, є дестабілізуючими факторами, оскільки вони впливають на інформаційний простір та обмежують доступ населення до своєчасної, надійної інформації. Це підриває довіру до інституцій через маніпуляції інформацією.

Важливо також підкреслити важливість ефективності кіберзахисту України в відбитті атак та/або пом'якшення їх впливу. Україна зміцнила стійкість своєї національної інфраструктура інформаційно-комунікаційних технологій (ІКТ) та реагування на кіберінциденти до та під час війни, у співпраці з урядами країн НАТО та приватними компаніями. Це включало заходи, спрямовані на посилення кіберстійкості України до та після військових вторгнень 2014 та 2022 років, а також співпраці з НАТО [22].

Критична інфраструктура була й залишається постійною ціллю в цій війні. Оскільки, всі основні послуги зараз багато в чому залежать від ІКТ та розробки й передачі інформації в режимі онлайн, існує яскраво виражений економічний і операційний вплив на організації та уряди, які є цільовими. Кібератаки та операції російської федерації є націлені на критично важливу інфраструктуру, що може мати серйозні наслідки для цивільного населення та може призвести до величезних втрат для людської безпеки, завдаючи шкоди постраждалим особам і громадам.

Інститут кібермиру зафіксував кібератаки та операції, здійснені 98 різними суб’єктам, станом на 31 травня 2023 року. З усіх кібератак, проаналізованих Інститутом, близько 80% є «самоорганізовані» атаки, під час яких суб'єкти загрози

публічно розкривають кібератаку та називають себе дійовою особою, що стоїть за нею. Цей аспект також вказує на ймовірне геополітичне значення цих атак. Наприклад, група хакерів KillNet, яку пов’язують з росією, проводила DDoS-атаки на охорону здоров'я у країнах, які підтримують Україну у війні з росією [17].

Кіберсфера дозволяє цілому ряду суб'єктів здійснювати атаки, що стосуються як держави, які знаходяться у війні, так і не воюючі держави. Ініційована урядом добровольча «кіберармія» стала помітним гравцем у російсько-українській війні. Ініційована українським урядом, ІТ-армія України є менш традиційним гравцем чиї DDoS-атаки сильно впливають на російські онлайн-ресурси [18].

Крім того, 2024 рік є роком виборів у десятках країн, де росія може спробувати втрутитися, намагаючись заручитися підтримкою своїх союзників або, як мінімум, відвернути від проукраїнських партій. У найменш дружніх країнах росія, швидше за все, продовжить просувати ідею – за допомогою більш таємних засобів – про те, що допомога Україні є чистою втратою для тих, хто проживає в цих країнах.

Справді, зусилля росії на сьогоднішній день досягли часткових результатів, таких як затримки з постачанням військової техніки, але вони не зупинили здатність України дати відсіч. Україна активно докладає зусиль для протидії російському впливу, виділяючи значні ресурси на моніторинг та протидію російським інформаційним операціям, і її успіхи на сьогоднішній день можуть дати світові певне уявлення про те, як протистояти зловмисному впливу.

З огляду на масштаби операцій росії та її очевидне бажання схилити світову громадську думку проти України, уряди в усьому світі, особливо ті, які сповідують демократичні цінності, повинні враховувати потенційні наслідки своїх рішень щодо України як такі, що в кінцевому підсумку є глобальними. Збільшення допомоги та допомоги Україні зміцнить глобальну демократію, тоді як її скорочення підірве не лише Україну, а й демократію в цілому.

3.2. Місце та вплив інформаційної війни в російсько-українській війні (2014-2024 рр.)

В Україні росія протягом останнього року прагнула підірвати волю країни до опору та посіяти внутрішній розбрат, дискредитуючи як цивільне, так і військове керівництво. Це включало зображення України як ненадійного союзника, посилення внутрішніх конфліктів та здійснення шахрайських атак на громадянське суспільство та звичайних користувачів. Наприклад, пропагандистський апарат Кремля налагодив найбільшу відому операцію впливу в TikTok для поширення чуток про українську політичну корупцію.

Всередині країни росія також спрямувала свої зусилля на контроль над внутрішньою аудиторією, насамперед зосередившись на обмеженні доступу до інформації. Такі інциденти, як заколот «Вагнера» у червні 2023 року, створили скрутне становище для Кремля щодо його толерантності до Telegram, який фактично служив цифровою домашньою базою для Євгена Пригожина та його колег-заколотників. Триваючі внутрішні заходи цензури та нагляду також зберігалися в російській федерації, включаючи законодавство про обмеження віртуальних приватних мереж (VPN), які використовуються для обходу обмежень в інтернеті. Федеральна служба росії з нагляду у сфері зв'язку, інформаційних технологій і засобів масової інформації, державний регулятор телекомунікацій, широко відомий як Роскомнагляд, також розгорнула систему інтернет-спостереження, відому як Oculus, призначену для виявлення контенту, який кремль вважає небажаним [23].

В **Європі** росія поширювала неодноразові заяви про те, що Україна продавала західну зброю для отримання прибутку на міжнародному чорному ринку, намагаючись підірвати європейську підтримку України. Росія також наполегливо просувала наратив про те, що країни-члени Європейського Союзу зіткнуться з труднощами взимку без доступу до російського газу, розгорнувши широку

інформаційну кампанію онлайн-впливу, що складається з понад п'ятдесяти фейкових веб-сайтів, які видають себе за авторитетні європейські ЗМІ.

Російські операції не обмежувалися тим, що європейські країни допомагали Україні зброєю та фінансовою підтримкою. Дослідники DFRLab спостерігали за тактикою цілеспрямованого обміну повідомленнями на Південному Кавказі та в Молдові, очевидно, з подвійною метою: підірвати підтримку України, одночасно розділяючи суспільства зсередини та отримуючи місцевий вплив. Наприклад, проросійські актори скористалися існуючою критикою прем'єр-міністра Вірменії Нікола Пашиняна після завоювання сусіднім Азербайджаном вірменського етнічного анклаву Нагірний Карабах; кремлівські чиновники, пропагандисти та інфлюенсери в Telegram розпалювали антиурядові настрої та закликали до повалення Пашиняна та його уряду.

В ***Азербайджані*** кремль скористався російськомовним впливом через академічні кола, обмінні курси та університети, використовуючи при цьому відсутність незалежних ЗМІ в країні.

У ***Грузії*** очолюваний «*Грузинською мрією*» уряд все ще прагне до розширення своїх відносини з росією як у політичному, так і в економічному плані після вторгнення в лютому 2022 року, використовуючи народні побоювання щодо ескалації війни в Грузії, щоб ще більше зміцнити проросійську позицію уряду.

В ***Молдові*** росія вдалася до енергетичного шантажу та розпалювання війни, посилюючи неправдивий наратив про те, що Молдова, Україна чи НАТО планують військову інтервенцію в підтримуваний росією сепаратистський регіон Придністров'я.

На ***Близькому Сході*** та в ***Північній Африці*** російські операції впливу спираються на медіа-імперію RT і Sputnik, а також на місцеві підсилювачі прокремлівських меседжів і широких анти-західних, антиколоніальних настроїв. В Африці росія застосовує подвійну стратегію: офіційний вимір, що включає торгівлю, інвестиції, дипломатію, зв'язки з громадськістю, оборонні угоди та взаємодію з

міжнародними організаціями, поряд з неофіційним та прихованим аспектом з використанням гібридних інструментів, тактики та таємної торгівлі зброєю за ресурси.

«*Основна увага приділялася неангломовній інформації в Африці*», – сказав Кайл Уолтер, керівник відділу досліджень Logically, компанії, яка відстежує дезінформацію та дезінформацію в Інтернеті. «*Вони широко йдуть по всьому спектру, як для того, щоб спробувати змінити свою думку про вторгнення, так і для того, щоб позиціонувати себе як кращого стратегічного партнера, який рухається вперед*»[1]. Під час прийняття різних резолюціях ООН особливо представники Африки та Південно-Східній Азії 15 із 20 країн регіону утримаються від голосування, і, можливо, дві-три фактично засуджують вторгнення росії в Україні [24].

У ***Латинській Америці*** RT і Sputnik служать каналами для російської комунікації, доповнюючись російськими послами і не афілійованими журналістами, які поширюють проросійську пропаганду.

Однак, росія зіткнулася з перешкодами у своїх інформаційних операціях. Після вторгнення великі американські соціальні мережі швидко почали позначати російські державні ЗМІ та обмежувати їхнє охоплення. Європейський Союз повністю заборонив RT і Sputnik, ще одного російського мовника. Facebook почав попереджати користувачів, коли вони натискали або намагалися поділитися посиланням з російського державного видання.

Проте, росія все ще полишає спроби перемогти в інформаційній війні проти України. Так, за словами представників Meta, оскільки великі платформи обмежили охоплення російських офіційних каналів, спостерігається сплеск таємної активності, пов'язаної з Росією. Минулого року компанія знищила дві великі мережі, намагаючись вплинути на сприйняття війни, залучивши понад 3000 облікових записів, сторінок і груп – це найбільші видалення операцій, пов'язаних з росією, з 2017 року. На відміну

1

від більш витончених зусиль впливу, які Meta фіксувала в минулому, компанія заявила, що тактика, яка використовується для націлювання на Україну, більше нагадує інструментарій спамерів: великий обсяг і низька якість.

«Ці кампанії нагадували операції з розгрому та захоплення, які використовували тисячі фальшивих облікових записів у соціальних мережах, а не лише на наших платформах, намагаючись перевантажити розмову контентом», – сказав Нік Клегг, президент Meta з глобальних справ [25].

У міру того, як російські меседж-кампанії поширюються в соціальних мережах, Кремль також розправляється всередині країни, блокуючи росіянам доступ до багатьох великих американських інтернет-платформ, включаючи Facebook і Twitter. Все це призводить до більш розколотого глобального Інтернету, де інформація, до якої ви піддаєтеся, все більше залежить від того, де ви знаходитесь у світі.

Дослідники очікують, що росія продовжить використовувати цю комбінацію тактик для просування своїх наративів – і використовувати ерозію довіри, якій вона сприяла протягом багатьох років.

«*Це грає на той факт, що все на даний момент є предметом обговорення», –* сказав Уолтер, дослідник Logically. «*Правда є предметом дебатів, демократія є предметом дебатів, наприклад, інституції та їхня роль у забезпеченні прав людини є предметом обговорення. Вони поставили все під сумнів*» [26].

Таким чином, Україна все ще повинна усвідомлювати, що інформаційна війна ще триває та вимагає значних зусиль для введення боротьби проти російської пропаганди та її наративів, оскільки російськи прихильники все ще намагаються зруйнувати глобальні позиції України, граючи в довгу гру, націлюючись на країни по всьому світу за допомогою дезінформаційних кампаній і кампаній впливу, спрямованих на зменшення громадської підтримки та готовності союзників надсилати допомогу до України.

Росія має довгу історію інформаційних операцій і операцій впливу по всьому світу, що робить її значним супротивником, який постійно прагне використовувати слабкості або проблеми у ворожих суспільствах. Так само росія зловживає ідеєю «нейтральних» ЗМІ для подачі своєї дезінформації поряд із висвітленням реальних подій, і все це з наміром створити у глядачів враження, що обидві версії подій заслуговують на увагу.

3.3. Засоби й механізми протидії інформаційній війні для забезпечення інформаційної безпеки в Україні

У відповідь на загрозу інформаційної війни держави створюють нові військові формування для проведення психологічних операцій, наприклад, британська армія створила два нових формування: 77-му бригаду для проведення психологічних операцій і 1-шу бригаду розвідки, спостереження і рекогносцировки, яка поєднує радіоелектронну боротьбу і розвідку ще в 2015 році. У звіті корпорації RAND наводиться аргумент на користь високоінтегрованого підходу до всіх аспектів інформаційної війни, щоб представити ефективні сили оборони. У США адмірал Майкл С. Роджерс оприлюднив заяву про бачення Кіберкомандування, в якій описав, як мають бути захищені мережі, системи та інформацію Міністерства оборони від кібератак і надаватиме підтримку військовим операціям і операціям у надзвичайних ситуаціях. Підхід США є більш інтегрованим, але це стосується лише збройних сил – з національної точки зору обом країнам бракує загального інтегрованого підходу зі спільною командною структурою, яка включає загрози цивільній інфраструктурі [27].

Отже, хоча концепція інформаційної війни здається добре зрозумілою, її аспекти не розглядаються разом, і таке розрізнене мислення може призвести до прогалин у світовій безпеці, що підсвітила російсько-українська війна. Західні уряди не змогли повною мірою усвідомити вразливість електронних комунікацій і величезні

ризики, які вони несуть для критичної інфраструктури, транспорту та безпеки цивільного населення. Директор американської розвідки наголосив на величезності кіберзагрози, з якою стикаються США, а британський генерал Ніколас Хоутон у своїй промові в Chatham House зауважив, що більшість актів фізичної війни сьогодні включають онлайн-аспект, коли соціальні мережі використовуються для маніпулювання думкою та сприйняттям. Британський генерал також визнав, що тактика, яку використовує Росія, поєднує в собі аспекти інформаційної війни, а також контррозвідки, шпигунства, економічної війни та спонсорування маріонеток таких як білоруська держава на чолі з Лукашенком Олександром Григоровичем.

Західним державам потрібно краще зрозуміти весь масштаб інформаційної війни, яку веде росія проти заходу в міру її розвитку, визначити, де ми найбільш вразливі, а потім створити єдину точку відповідальності для впровадження захисних механізмів. Тому що російська федерація, яка не обмежена ні західною політикою, ні етичними чи правовими кодексами, може і буде використовувати західні вразливі місця.

Дослідники розглядають три можливі сценарії розвитку, які може використати росія проти України: (I) кіберпатова ситуація: росія намагається інтегрувати кібернетичні та звичайні ефекти на полі бою та за його межами через стійкість кіберзахисту, а також силу державно-приватного партнерства; (II) росія перегруповується і запускає хвилю кібератак на критично важливу інфраструктуру США; (III) цифрова брехня: російські операції впливу за допомогою кібертехнологій та комп'ютерна пропаганда знижують підтримку Сполучених Штатів та війни в Україні [28].

Розгляд цих сценаріїв свідчить про ключові варіанти політики, кожен з яких узгоджується з активною кампанією та інтегрованим стримуванням, адміністрація Байдена може взяти на себе протягом наступних двох років, щоб сформувати те, що, ймовірно, буде довгостроковою конкуренцією з росією, яка простягнеться глибше в

XXI століття. З часом стало зрозуміло, що стійкість і зосередженість на оборонних операціях можуть запобігти потенційним наслідкам наступальних кібероперацій. Захист у кіберпросторі вимагає розширення державно-приватного партнерства та співпраці поряд з об'єднаними даними для виявлення моделей і тенденцій атак.

Також, Сполученим Штатам та їхнім партнерам потрібно буде розробити кращі шляхи та засоби протидії тому, як зловмисні суб'єкти, такі як росія, використовують кіберпростір для спотворення глобальної громадської думки. На кожне невдале вторгнення в мережу припадають тисячі успішних публікацій у соціальних мережах, які спотворюють те, як світ дивиться на війну в Україні.

Таким чином, як зазначалося вище, кібератаки є все ще сучасними загрозами під час російсько-української війни. На протидії цій загрозі, український уряд, зокрема 26 лютого 2022 року Міністерство Цифрової трансформації України оголосили конкурс до армії ІТ-спеціалістів для боротьби за Україну в кіберпростірі. Цей заклик був унікальним для держави в ситуації збройного конфлікту і мав на меті залучити українських талантів *«продовжити боротьбу на цифровому фронті».* Звертаючись до українців, у контексті глобального протесту проти вторгнення росії та військових нападів на цивільне населення, заклик, призвів до участі людей з усього світу [29].

Крім того, застосування кіберзасобів та інформаційних операцій у російсько-українській війні ставить серйозні виклики для державних і приватних суб'єктів щодо правил і положень, що застосовуються до кібератак. Кібератаки та інформаційні операції під час збройних конфліктів не відбуваються в правовому вакуумі. Реальність використання кіберпростору проти критично важливої інфраструктури викликає серйозне занепокоєння щодо того, як держави поважають і дотримуються існуючої правової бази. Кібероперації самі по собі не є «незаконними» відповідно до міжнародного права, але можуть розглядатися як такі, якщо вони спричиняють наслідки, що порушують міжнародне право зобов'язань. Критичною прогалиною є відсутність згоди щодо того, як застосовується міжнародне право.

Щоб закрити цю прогалину, держави повинні домовитися про чіткі правила своєї відповідальності відповідно до міжнародного гуманітарного право, визначивши, як ці принципи застосовуються до використання ІКТ і до операцій в умовах збройних конфліктів. Цим роз'яснення слід також враховувати Римський статут, який особливо актуальний для залучення нетрадиційних суб'єктів, оскільки саме він накладає обов'язок кожної держави здійснювати свою кримінальну юрисдикцію щодо осіб, відповідальних за міжнародні злочини. Є кілька способів, на якими необхідно працювати над побудовою спільного розуміння щодо притягнення до відповідальності за зловмисне використання кібернетики, у тому числі через заяви урядів та держав. Держави також можуть активно роз'яснювати, коли і як відбулося порушення міжнародного права, наприклад, коли санкції накладаються або коли здійснюються політичні атрибуції.

Крім того, поточні політичні та правові заходи потребують подальших роз'яснень, оскільки не є ефективним вирішення цих проблем. Наприклад, кіберінструменти можуть мати подвійне призначення технології військового та цивільного призначення, що додає додатковий рівень складності. Неповний перелік необхідних роз'яснень включає встановлення того, що є *«нападом», «шкодою», «об'єктом», «військова мета»* та *«кримінальна відповідальність»* у кіберпросторі, а також відсутність консенсусу щодо конкретних реакції на різні типи атак.

Таким чином, розроблення правового регулювання, зокрема притягнення до відповідальності за кіберзлочини під час війни на міжнародному рівні також потребує уваги та розробки. Належне правове регулювання, зокрема механізм притягнення до відповідальності суб’єктів за вчинення кібератак проти інших держав з метою повалення їх державного устрою, створення загроз національній безпеці може стати одним із заходів протидії під час російсько-української війни. Крім того, США повинні усунути свої недоліки з різних напрямків, якщо вони хочуть повернути стратегічної переваги або навіть успішно захищатися від російських форм і тактики.

Необхідно також зміцнювати зв'язки між державами, які є обов'язковими для захисту та оборони. Стратегії, орієнтовані на людину, повинні виявляти та руйнувати людські мережі, які беруть участь у поширенні, створення мереж для запуску кампаній російської федерації інформаційних війн, а також сприяння розробки довготривалих і потужних заходів контррозвідки. З точки зору контррозвідки – це означає виявлення зв'язків між тими, хто перебуває в циклі прийняття рішень, і зовнішніми суб'єктами, такими які пов'язані з Кремлем аналітичними центрами та стейкхолдерами, на яких чиниться тиск під час кампаній інформаційної війни через незаконне фінансування та інвестиції [30].

Розвідувальне співтовариство США разом з Україною має націлитися на російські установи, які надають основам розвитку російської доктрини інформаційної війни. Наприклад, один широко зрозумілий елементом ефективного рефлексивного контролю є заохочення непередбачуваності.

Консолідація та координація зусиль США та Україна. США разом з Україною повинні розвивати професіоналізм людського капіталу, а потім децентралізувати та розпорошити реалізацію стратегічних цілей через цих осіб. Крім того, розгляд створення робочої групи з активних заходів (AMWG) для виявлення російської дезінформації є необхідним. Організація зможе «виявляти та викривати» російську дезінформацію і може бути засекреченою та загальнодоступною версією.

Контрпропаганда України має висвітлювати антилібералізм росії щодо певних груп населення, корумпованість російських еліт та олігархів, посилення дисидентських історій у росії, і потенційне використання православною громадою, яка сьогодні тісно пов'язана з російською державою.

Пріоритетом у боротьбі з тактикою, особливо дезінформацією та полемікою, має бути збалансований більше, ніж врівноважений. Об'єктивність і стійкість повинні бути двома найважливішими методами боротьби з російською інформаційною війною. Українське суспільство, яке зазнає нападу, має пережити нинішній хаос з

терпінням і сили духу, поки не будуть знайдені факти. На жаль, нинішні засоби масового характеру комунікації в Україні не завжди породжують заходи стійкості та об'єктивності.

Ведення інформаційної війни є можливим, зокрема, через відсутність індивідуальної безпеки, що забезпечується поточними регуляторними заходами в цифровому просторі. Дані, які зібрані про фізичну особу, які уряд США не може використовувати, є часто продані та використанні супротивниками для запуску кампаній інформаційної війни російської федерації, щоб переконати або змінити індивідуальну особу. Регулювання того, хто може збирати персональні дані, тривалість їх зберігання та способи й правила зберігання, а також як можливі способи розповсюдження даних, є ключовими способами регулювання держави. Тобто, забезпечення високих стандартів конфіденційності та захисту персональних даних є пріоритетним завданням України та США.

ВИСНОВКИ

Перша згадка та визначення «інформаційна війна» (information warfare) з’явилося ще в середині 1980 років після завершення холодної війни між СРСР з однієї сторони та Західної Європи та США з іншої сторони, що зумовило виникнення нових завдань перед Збройними силам. «Інформаційну війну» можна визначати як форму протистояння або протиборства між державами або неурядовими, політичними, економічними або іншими структурами, що реалізується з метою завдати шкоди інформаційній сфері опонента та забезпечити захист власної інформаційної безпеки.

До основних моделей організації інформаційної війни можна віднести: модель нейтралізації, модель пропагандистської комунікації, модель масової комунікації, модель резонансного впливу, семіотичну модель, модель дезінформації та модель масової демонстрації організації інформаційного впливу.

Інформаційна війна безперервно здійснюється росією проти України з метою усунення української влади та приведення до влади «проросійських» політиків, що виступатимуть «маріонетковим корпусом управління» та контролюватися політичним управлінням російської федерації. Як проаналізовано в цій роботі росія використовує інформаційні кампанії як підготовку для подальшого безпосереднього ведення військових операцій, зокрема міцного підґрунтя.

До основних принципів інформаційної війни можна віднести: (I) відмова, (II) посилення сили, (III) виживання, (IV) ситуаційна обізнаність, командування, контроль; (V) комунікації та їх рівень.

Таким чином, метою російської інформаційної війни є не тільки створення та безпосереднє ведення війни. Це підготовка ґрунту та знаряддя тиску під час війни, які допомагають веденню безпосереднього ведення війни. Мета інформаційної війни не переконувати нікого в правді, вона повинна породжувати шум і руйнувати ідею об'єктивної істини. По суті, все зводиться до переконання тих, кого можете, і збивати

з пантелику тих, кого не можете. Наративи росії є небезпечними для споживання їх українським суспільством та іншими демократичними суспільствами. Кожен інструмент, який використовуються росіянами, це один з аспектів кумулятивної, довготривалої кампанії зі створення, спрямування та підтримки особливої рамки, які вигідні геополітичним цілям росії.

У відповідь на інформаційну війну, яку веде росія проти України, країни – члени Європейського Союзу, США, Великобританія, інші країни повинні створювати нові військові формування для проведення психологічних інформаційних операцій та розвідки, спостереження і рекогносцировки, яка буде поєднувати радіоелектронну боротьбу і розвідку. Не слід недооцінювати росію, оскільки вона має потужні інструмент та досвід у введенні інформаційних воїн, які реалізуються, зокрема, шляхом їх жахливої та небезпечної пропаганди, яка працює як на російське суспільство, так і на українське суспільство.

Україні разом із США, країнами Європейського Союзу потрібно бути готовими до довготривалого протистояння з росією не тільки в військовому конфлікті, але й в інформаційному полі. Розробляти заходи та стандарти безпеки з метою забезпечення належного рівня захисту та конфіденційності, інформаційної безпеки індивідуальної особи та інформаційної мережі держави в цілому.

Контрпропаганда України має працювати на захист інтересів України та забезпечення національної безпеки, зокрема висвітлювати та підкреслювати правдиву інформацію про реальний стан речей, при умові, що це не суперечить національній безпеці України. Крім того, висвітлювати антилібералізм Росії щодо певних груп населення, корумпованість російських еліт та олігархів. Тобто, дискредитувати дії та політику російського правління, яку здійснює російська федерація проти України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аналіз Міжнародного економічного форуму. Що таке інформаційна війна? 3 грудня 2015. URL: https://www.weforum.org/agenda/2015/12/what-is-information-warfare/.
2. Мирний В.В., Мороз А.С. Інформаційна війна. // Велика українська енциклопедія. URL: https://vue.gov.ua/Інформаційна війна
3. Директива Департаменту Захисту № S-3600-1 від 9 грудня 1996 року. URL: https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Other/14-F-0492_doc_02_Directive_S-3600-1.pdf.
4. Margaret Rouse. What is Information Warfare? Definition from Techopedia. URL: https://www.techopedia.com/definition/29777/information-warfare.
5. Stein G.J. AWC INFORMATION WARFARE [Electronic resource] / George J. Stein. ULR: https://universityofleeds.github.io/philtaylorpapers/vp01e61f.html
6. Стадник А.Г. Основні моделі організації інформаційних війн та їх різновиди. Соціальні технології: актуальні проблеми теорії та практики, 2015, вип. 67-68. URL: http://soctech-journal.kpu.zp.ua/archive/2015/67-68/11.pdf.
7. World Economic Forum. What is information warfare and how pervasive is it? | World Economic Forum. 14 April 2022. URL: https://www.weforum.org/agenda/2022/04/what-is-information-warfare-and-how-pervasive-is-it/
8. Martin Libicki, What is Information Warfare, National Defense University, 1995. URL: https://apps.dtic.mil/sti/pdfs/ADA367662.pdf
9. Dorothy E. Denning, Information Warfare and Security, Addison-Wesley, 1999. URL: https://priv.gg/e/Information%20warfare%20and%20security.pdf

10. Daniel E Magsig, Information Warfare In The Information Age, 1996. URL: https://books.google.it/books/about/Information_Warfare_in_the_Age_of_Cyber.html?id=Z2LyDwAAQBAJ&redir_esc=y
11. Russel Deborah and Gangemi G.T., Computer Security Basics, (O'Reilly & Associates, 1994). URL: https://archive.org/details/computersecurity00russ/page/n5/mode/2up .
12. Propaganda and information warfare as socio-philosophical phenomena and political tools, synesis. Universidade Católica de Petrópolis, Rio de Janeiro, Brasil v. 15, n.3, 2023. URL: https://seer.ucp.br/seer/index.php/synesis/article/download/2599/3551/10505
13. Анатомія російсько-українського конфлікту (2014–2022 рр.) в епоху гібридних війн URL: http://www.nbuv.gov.ua/node/5937.
14. Мележик О. О. Світова гібридна війна: український фронт / О.О. Мележик // Вісн. НАН України. 2017. № 2. С. 3-8
15. Мідттун Г.П. Битва умів. Гібридна війна – це вплив на людей, з метою підвести їх до свідомого чи не свідомого вибору, корисного для агресора URL: https://bit.ly/3NlibMR
16. Harrold D. Lasswell Пропагандистська техніка під час Другої Світової Війни. URL:https://books.google.com.ua/books?id=3yeODwAAQBAJ&printsec=frontcover&hl=uk&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
17. Computer Weekly, 'Russian DDoS hacktivists seen targeting western hospitals', 31 January 2023. URL: https://www.computerweekly.com/news/365529957/Russian-DDoS-hacktivists-seen-targeting-western-hospitals.
18. Stéphane Duguin. CyberPeace Institute. 'How an armed conflict is destabilizing cyberspace for us all', 11 November 2022. URL: https://cyberpeaceinstitute.org/news/how-armed-conflict-is-destabilizing-cyberspace/.

19. Russian information war against Ukraine: peculiarities and mechanisms of countering (Review Article) SHV. 2018 Volume 4, Number 1:55-62 URL: https://doi.org/10.23939/shv2018.01.055.
20. Тамбіама Мадьєга. Війна Росії проти України: цифровий вимір РВВ / Європейська парламентська дослідницька служба. Дослідницька служба членів PE 729.317 березень 2022 року URL: https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/729317/EPRS_ATA(2022)729317_EN.pdf.
21. Підрив України: як росія розширила глобальну інформаційну війну у 2023 році. Дослідження Лабораторія цифрових криміналістичних досліджень. URL: https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/.
22. Стефан Дюген, Павліна Павлова. Роль кібернетики у війні Росії проти України: його вплив та наслідки для майбутніх збройних конфліктів. PE 702.594 вересень 2023 URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf
23. Абрамов В.І. Гібридна війна як нова форма міждержавного протиборства: стратегія перемоги. Виклики і загрози національній безпеці в умовах гібридної війни : матеріали наук.-практ. семінару (Київ, 27 квітня 2017 р.) К.: НАДУ, 2017. С. 17-22.
24. Інформаційно-психологічне протиборство (еволюція та сучасність): монографія / Я.М. Жарков, В.М. Петрик, М.М. Присяжнюк та ін. К.: ПАТ «Віпол», 2013. 248 с.
25. Магда Є.В. Гібридна війна: вижити і перемогти. Х.: Віват, 2015. 304 с.
26. Панчук Д.М. Зброя інформаційна/ // Велика українська енциклопедія. URL: https://vue.gov.ua/Зброя інформаційна.

27. Кравчук О.Ю. Інформаційна війна проти країни як індикатор рівня забезпечення політичної безпеки. Регіональні студії, 2020. URL: http://regionalstudies.uzhnu.uz.ua/archive/20/21.pdf
28. Галамба М. Сутність, види та методи спеціальних інформаційних операцій. Юридичний журнал. К.: Юстініан, 2007. URL: https://mydocx.ru/12-95476.html.
29. Почепцов Г. Росія і Україна у співставленні їх комунікативно-пропагандистських можливостей. URL: https://ms.detector.media/manipulyatsii/post/52/2014-08-03-rosiya-i-ukraina-u-spivstavlenni-ikh-komunikativnopropagandistskikh-mozhlivostei/ .
30. Прокоф'єв Д.М. Інформаційна війна та інформаційна злочинність. Вісник Запорізького юридичного інституту. 2000. №1, С. 288-307.