

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ПОПНЕЦЬ ІННА ІГОРІВНА

Допускається до захисту:
в.о. завідувача кафедри
міжнародних відносин і зовнішньої політики,
к.і.н., доцент
_____ І.В. Богінська
« _____ » _____ 2021 р.

ІНФОРМАЦІЙНА ВІЙНА РОСІЇ ПРОТИ УКРАЇНИ

Спеціальність 291 Міжнародні відносини, суспільні комунікації та
регіональні студії

Кваліфікаційна (бакалаврська) робота

Керівник:

Котик Ю. В. старший викладач
кафедри міжнародних відносин
і зовнішньої політики, к.і.н.

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

Голова ЕК: _____
(підпис)

АНОТАЦІЯ

Попінець І. І. Інформаційна війна Росії проти України. Спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії». Донецький національний університет імені Василя Стуса, Вінниця, 2021.

У кваліфікаційній (бакалаврській роботі) досліджено природу та трансформацію інформаційних війн. Показано особливості інформаційної війни Росії проти України. Визначено методи протидії в українському контексті.

Ключові слова: інформаційна війна, національна безпека, інформаційна загроза, кібербезпека.

ABSTRACT

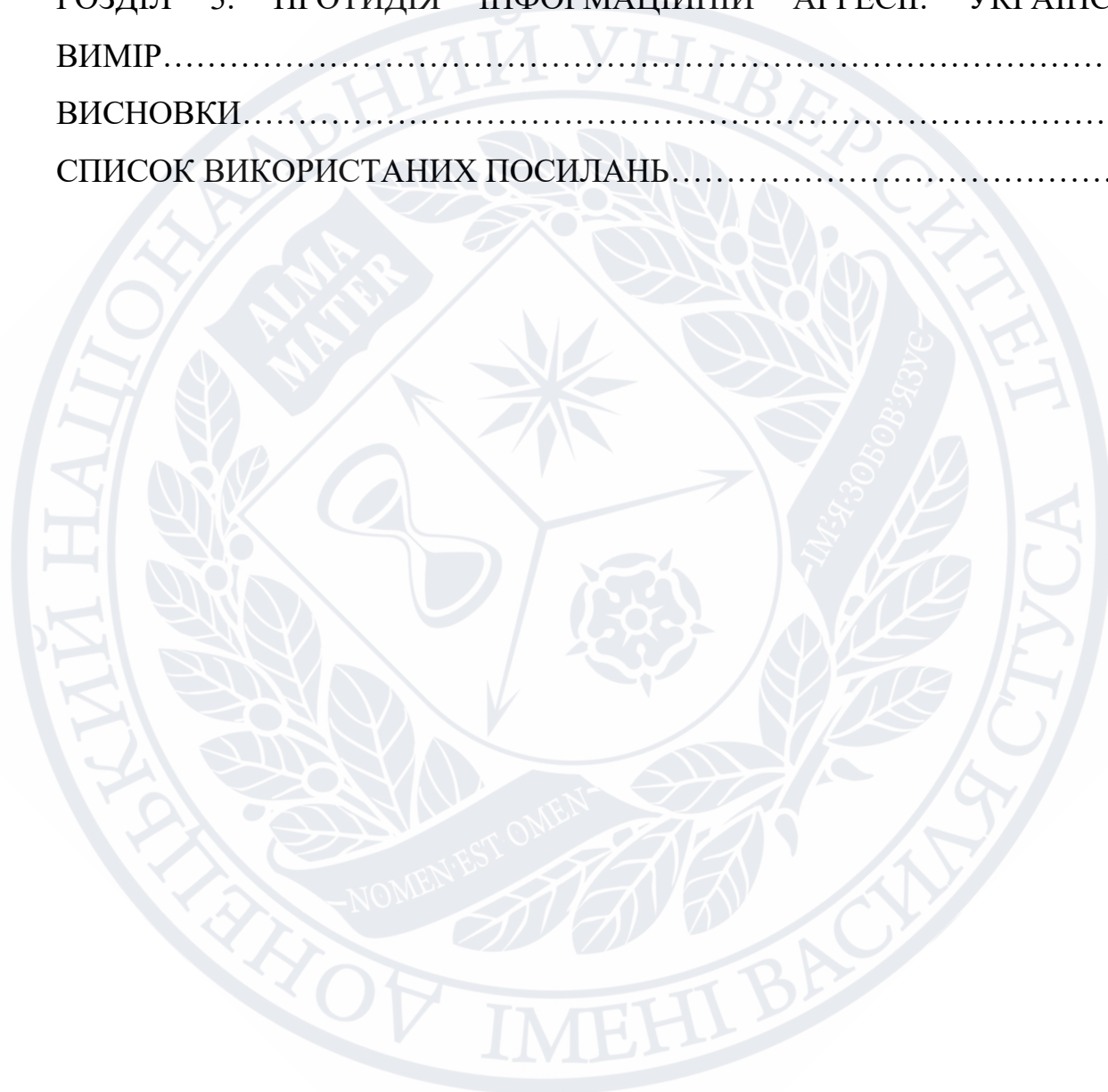
Popinets I. I. Information war of Russia against Ukraine. Specialty 291 "International Relations, Public Communications and Regional Studies". Vasyl Stus Donetsk National University, Vinnytsia, 2021.

The nature and transformation of information wars are studied in the qualification (bachelor's work). The peculiarities of Russia's information war against Ukraine are shown. Methods of counteraction in the Ukrainian context are defined.

Key words: information war, national security, information threat, cybersecurity.

ЗМІСТ

ВСТУП.....	3
РОЗДІЛ 1. ПРИРОДА ТА ТРАНСФОРМАЦІЯ ІНФОРМАЦІЙНИХ ВІЙН.....	6
РОЗДІЛ 2. ОСОБЛИВОСТІ ІНФОРМАЦІЙНОЇ ВІЙНИ РОСІЇ ПРОТИ УКРАЇНИ.....	20
РОЗДІЛ 3. ПРОТИДІЯ ІНФОРМАЦІЙНІЙ АГРЕСІЇ: УКРАЇНСЬКИЙ ВИМІР.....	39
ВИСНОВКИ.....	53
СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ.....	55



ВСТУП

Актуальність теми дослідження. Досвід інформаційного протистояння України та Росії показує, що вітчизняні структури з інформування населення, на відміну від ворожих російських, де кожна атака ретельно планується, не відрізняються особливою підготовкою чи усвідомленістю в питаннях кібербезпеки чи антипропаганди. В сучасному світі потрібно зважати на потенціал використання інформаційних мереж у воєнних цілях. На сучасному етапі розвитку системи кібербезпеки України варто приділити увагу дослідженню основних причин вразливості інформаційної сфери України та актуальних і дієвих методів протидії інформаційній агресії. Для успішного розв'язання поставлених завдань було використано методи індукції та дедукції, порівняльного аналізу, описово-аналітичний із дотриманням принципів об'єктивності та історизму.

Мета дослідження – дослідити природу та трансформацію інформаційних війн у контексті протистояння Росії і України.

Завдання дослідження полягає у вивченні та аналізі природи та історичної трансформації інформаційних війн; виявленні особливостей інформаційної війни між Україною та Росією; з'ясуванні причини, чому дії країни-агресора, були результативними; визначенні особливостей протидії інформаційній агресії в українському вимірі.

Об'єкт дослідження – інформаційна війна як елемент гібридної війни у ХХІ ст.

Предмет дослідження – особливості ведення інформаційної війни Росії проти України.

Теоретичне значення одержаних результатів. Дослідження історичного розвитку інформаційних війн та їх трансформації дозволяє зрозуміти природу та небезпеку, що несуть в собі гібридні інформаційні війни. Проаналізувавши особливості інформаційної війни Росії проти України, виявлено основні методи, що використовувалися ворожими силами. Розуміння техніки ведення інформаційної війни дозволяє розробити ефективну систему протидії.

Доведено, що найважливішими заходами протидії є: ефективна комунікація між владними структурами та суспільством, підвищення якості журналістики та довіри людей до неї, розробка та впровадження новітніх конкурентоспроможних засобів кіберзахисту.

За допомогою методу комплексної оцінки впливу ворожих інформаційних атак на Україну було проаналізовано основні кібербезпекові загрози та запропоновані варіанти протидії кіберагресії, що забезпечують національну безпеку країни та відображають інтереси України.

Апробація результатів дослідження.

Попінець І. Інформаційна війна як загроза національній безпеці держави в ХХІ ст. [Електронний ресурс] / Інна Попінець // Збірник матеріалів Міжнародної наукової конференції «Травневі студії 2021: історія, міжнародні відносини» Донецький Національний Університет ім. Василя Стуса. Вип. 5. 58

Структура кваліфікаційної (бакалаврської) роботи. Кваліфікаційна робота складається з: вступу, трьох розділів, висновків, списку використаних джерел із 41 найменувань. У тексті бакалаврської роботи міститься 1 таблиця. Загальний обсяг роботи 54 аркуші.

РОЗДІЛ 1. ПРИРОДА ТА ТРАНСФОРМАЦІЯ ІНФОРМАЦІЙНИХ

Використання інформаційно-комунікаційних технологій у сценаріях воєн було головним інтересом урядів, спецслужб та експертів з питань безпеки протягом останніх двох десятиліть. Цьому сприяв швидкий розвиток та поширення інформаційних технологій, їхня всеосяжність та відсутність фізичних кордонів між країнами в інформаційному просторі. За допомогою методу комплексної оцінки впливу ворожих інформаційних атак на Україну було проаналізовано основні кібербезпекові загрози та запропоновані варіанти протидії кіберагресії, що забезпечують національну безпеку країни та відображають інтереси України.

Вивченням проблеми інформаційних війн займалися багато зарубіжних вчених, серед яких найвідомішими стали – М. Лібікі, Е. Тоффлер, Г. Кіссінджер. Серед вітчизняних науковців найвагоміший вклад у дослідження цієї проблеми зробили: С. Грін'єв, О. Калиновський, А. Крутських, І. Панарін, Г. Почепцов.

Існує велика кількість невійськових дій, які за своєю ефективністю можуть зрівнятися з кінетичними. І найбільш наближеною до них по безлічі своїх функцій є інформаційна зброя, застосування якої населення не відчуває. Інформація здається безпечною, вона не стріляє і не вибухає. Але це тільки в фізичному просторі. В інформаційному і віртуальному просторах вона несе руйнування і непоправні наслідки. Зберігаючи в незмінності фізичне тіло, вона успішно діє на «приймач інформації» - людський розум.

Перш ніж аналізувати різні визначення інформаційної війни, відзначимо її важливу властивість: ведення інформаційної війни не буває випадковим чи відособленим, а передбачає узгоджену діяльність із використанням інформації, як зброї для ведення бойових дій як на реальному полі бою, так і у економічній, політичній, соціальній сферах.

Погляди щодо того, коли саме вперше було вжито поняття «інформаційна війна» різняться, тому важко визначити хто вигадав цей термін, та коли його було вперше вжито.

На думку І.М. Панаріна, вперше термін «інформаційна війна» був ужитий в 1967 році А. Даллесом в книзі «Таємна капітуляція», де йдеться про таємні переговори між США та Великобританією з одного боку та рейхсфюрером СС Генріхом Гімлером – з іншого. Пізніше це поняття часто вживається в пресі [13].

Також класичним прикладом інформаційного протистояння можна вважати Холодну війну (1946-1991рр). всім відомо, що вона не містила елементів збройного протистояння сторін. Конфронтація відбувалася на інформаційному та психологічному (агітації, пропаганда тощо) рівнях.

М. Маклюен у 60-х роках ХХ ст. одним з перших в відкритому друці написав про інформаційні війни [19]. Він вже тоді розумів, що холодна війна ведеться за допомогою інформаційних технологій.

Поняття інформаційної війни пройшло велику історичну трансформацію. Кожне покоління науковців в певній мірі досліджували інформаційні аспекти війни, але саме поняття було окреслене та сформульоване лише у ХХ ст. з розвитком інформаційних технологій, поширення засобів комунікації між людьми на всій земній кулі.

Тобто, якби не інформаційна революція, поняття інформаційної війни ніколи б не вийшло в розряд окремого виду протистояння, адже інформаційний простір не має фізичних кордонів і може обійтись без збройного втручання. Тоді, в поняття класичної війни, входили б методи інформаційного протиборства (пропаганда, дезінформація т.ін.), але не було б такого окремого виду війни, як інформаційна.

Для більш чіткого розуміння природи та сутності інформаційних війн важливо розуміти сутність цього поняття. Сьогодні існує багато різних трактувань поняття «Інформаційна війна». Перш за все це пов'язано з варіаціями перекладу словосполучення «information warfare». Його переводять і

як «інформаційна війна», і як «інформаційне протиборство», і як «інформаційно-психологічна війна».

Розглянемо різні варіації тлумачення цього поняття, щоб краще зрозуміти його природу:

- Расторгуєв С. П. вважає, що інформаційна війна це - відкриті і приховані цілеспрямовані інформаційні впливи систем один на одного з метою отримання певного виграшу в матеріальній сфері [22]. Це визначення ясно дає зрозуміти основні елементи інформаційної війни, що виділяють її як особливий вид гібридної війни.

- Строувел Д. визначає інформаційне протиборство як суперництво між соціальними системами (країн, блоків країн) в інформаційній сфері з приводу впливу на ті або інші сфери соціальних відносин і встановлення контролю над джерелами стратегічних ресурсів, у результаті якого одна група учасників суперництва отримує переваги, необхідні їм для подальшого розвитку [37].

- Інформаційно-психологічна війна - психологічний вплив на війська (сили) противника і населення з метою їх деморалізації і схиляння до припинення опору [37]. Проаналізувавши дані визначення варіацій перекладу терміну «information warfare», можна зробити висновки про основні характерні риси інформаційної війни:

- Не завдає фізичних руйнувань, що може призвести до запізнення у відповідній реакції;
- Не несе фактичних людських жертв з жодної сторони конфлікту;
- Відволікає увагу супротивника від важливого на другорядне;
- Покладається на керування громадською думкою та свідомістю заради переваги у протистоянні (навіть фактично супротивник, що програв, в очах суспільства може покращити своє становище за допомогою дезінформації);

- За необхідності, будь-які правдиві факти та судження нівелюються, дискусії зводяться до абсурду та ін.

Мартін Лібікі визначає сім видів інформаційної війни [32]:

- командно-управлінська - ставить перед собою мету позбавити контролю налагоджений зв'язок між командуванням і виконавцем;
- розвідувальна війна - передбачає збір цінної інформації для нападу і власного захисту;
- електронна війна - метою є виведення з ладу всіх електронних комунікацій;
- психологічна війна - пропаганда і інформаційне зомбування населення;
- хакерська війна - злом і доступ до будь-яких даних (електронна пошта, банківські картки, особисті файли, листування і так далі) і несанкціоноване їх використання;
- економічна війна - інформаційна блокада (обмеження комерційної діяльності) або інформаційний імперіалізм (політична інформаційна атака);
- кібервійна - ставить перед собою мету захопити комп'ютерні дані, вистежити об'єкт, порушити роботу інфраструктури, яку належить мати інформаційні технології [28].

Виходячи з описаних вище характерних рис інформаційної війни, можна сформулювати оптимальне визначення: інформаційна війна – це вплив на людину або групу людей завідомо неправдивою інформацією заради власної вигоди.

Дослідивши та проаналізувавши поняття інформаційної війни, можна чітко побачити який вплив на національну безпеку може мати застосування методів інформаційного протистояння, особливо за умови цілеспрямованого та комплексного підходу.

Різні автори дають різні визначення інформаційної війни:

- згідно з визначенням Манойло А. В. інформаційна війна – це процес протиборства людських спільнот, спрямований на досягнення політичних, економічних, військових чи інших цілей стратегічного рівня, шляхом впливу на цивільне населення, влади і (або) збройні сили протилежної сторони, за допомогою розповсюдження спеціально відібраної і підготовленої інформації, інформаційних матеріалів, і, протидії таким діям на власну бік [6].

- Згідно з працею Георгія Почепцова, представлено визначення інформаційної війни як такої, що має наступальні і оборонні складові, яка починається з цільового проектування та розробки своєї «Архітектури командування, управління, комунікацій, комп'ютерів і розвідки», що забезпечує особам, які приймають рішення, відчутну інформаційну перевагу у всіляких конфліктах [19].

- М. Маклюен визначає інформаційну війну як явні і приховані цілеспрямовані інформаційні впливи систем один на одного з метою отримання певного виграшу в матеріальній сфері [19].

Явище інформаційних війн існувало так чи інакше з давніх часів. Здійснення інформаційних впливів з використанням інформаційної зброї (приховування інформації; подача її частково, у певному ракурсі; перебільшення наслідків) було зафіксовано літописцями на територіях сучасної України ще за Київської Русі.

Спроби впливати за допомогою інформації на свідомість людини простежуються ще в працях Н. Макіавеллі – «Государ» або Сунь Цзи – «Мистецтво війни». У будь-які часи завжди цінувалося вміння зібрати якісну інформацію і ввести противника в оману.

До прикладу, загальновідомим є факт поїздки княгині Ольги до Константинополя, проте ні візантійські, ні руські джерела не вказують причину та мету такої довгої подорожі. Войовничий князь Святослав заздалегідь повідомляв противника про початок військових дій, проте залишав у таємниці напрям та сили, котрі планувалося залучити. Це давало можливість навести паніку у стані військ та швидко розгромити противника [17].

Явище інформаційної війни в історії людства не ново; російські дослідники А. Д. Васильєв і Ф. Е. Подсохін пишуть у зв'язку з цим: «античні автори у всіх фарбах описували агітаційні кампанії, що деморалізують і таким чином ослабляють противника, або навпаки - піднімають бойовий дух співвітчизників» [17].

Загальновідомою є біблійська історія про Гедеона, який залякував своїх ворогів під час воєн для того, щоб дестабілізувати їх воєнний дух. Згадується, що одного разу армія його противника була настільки розгублена та деморалізована чутками про розмір та войовничість ворожого війська, що вони вдарили по своїх військах.

Прояви інформаційної пропаганди було зафіксовано під час Кримської війни (1853-1856), коли відразу після Синопської битви англійські газети у звітах про бої писали, що російські військові нібито дострілювали поранених турків, що плавали в морі [39].

Активно велася інформаційна війна і в роки Першої світової війни 1914 - 1918 рр., в тому числі на Російському фронті. Прикладом цього може служити приховування реальної кількості солдат та зброї у розпорядженні 8-ї армії, що знаходилась під розпорядженням генерала-фельдмаршала П. фон Гінденбурга. Іншим прикладом є книга «Прориви російсько-карпатського фронту біля Горлиці - Тарнова в 1915р», де автор постійно згадує про «міцно укріплені російські позиції» та «величезні російські сили». Але було абсолютно навпаки – в жодній операції Першої світової війне не спостерігалось такої сильної переваги австро-німецьких військ над супротивником. Вони переважали російську армію в 2,5 рази в людській силі та в кількості кулеметів, а також в 4 рази в легкій, та в 40 разів у важкій артилерії [20].

Проте, поняття інформаційної війни з'явилося відносно недавно – коли інформаційні методи суспільно-політичної (протидії) дії отримали вкрай широке поширення, а соціальні дослідження досягли певного прогресу.

Інформаційна війна набула особливо важливого значення у XX ст. з початком розвитку засобів масової комунікації: газети, радіо та телебачення, тоді інформація, що поширювалася через них стала справді масовою.

Саме в цей час, коли засоби масової інформації набувають все більшого значення, інформаційні війни перестають бути доповненням до збройних, і стають самостійним видом протистояння. До прикладу, німецько-австрійська радіовійна 1933-34 рр. з приводу приєднання Австрії до рейху. Саме тоді вперше з'являється термін «інформаційний агресор».

Отже, розглянувши деякі історичні аспекти розвитку інформаційних війн, можна зробити висновок, що певні прийоми інформаційних воєн використовувалися з давніх-давен, хоча саме поняття інформаційної війни було сформовано лише в середині XX ст., з появою та розвитком інформаційних технологій. Значного розвитку це поняття зазнало за часів «холодної війни». Це період конфронтації, що не супроводжувався силовим вирішенням конфлікту, що цілком відповідає опису інформаційної війни. В цей час великого значення набувають публікації преси, телебачення та кінематограф, що активно розвивався в США та пропагував американські цінності. Думка громадськості була вкрай важливою, що змушувало країни вдаватися до різних хитрощів, щоб показати переваги свого життєвого укладу.

Інформаційні війни являються одним з видів гібридних війн. Гібридними називають війни, що не обмежені якимось одним аспектом воєнних дій. Часто це агресія з прихованими намірами, що проявляється через відмінні від силових методи, а саме через суб'єктів, організації з комплексним застосуванням політичних, економічних, інформаційних та інших невійськових заходів, а також терористичні, диверсійні, підривні та інформаційні технології.

Концепція гібридної війни не є особливо новою, вона представляє собою поєднання звичайної та нетрадиційної нерегулярної війни, що виходить за межі поля бою і охоплює економічну, дипломатичну, інформаційну (зокрема психологічну та дезінформаційну) та політичну війну.

Поняття гібридної війни досі не введено в українське законодавство, що робить майже не можливим формування комплексної моделі на юридичному та політичному рівнях. Можливо це поняття ще достатньо нове і не отримало достатньо сформованого визначення в наукових колах, але певні риси та особливості уже сформовані та визначені.

Не існує загальновизнаного визначення гібридної війни; деякі дискутують, чи термін взагалі корисний. Абстрактність цього терміну означає, що він часто використовується як загальний термін для всіх нелінійних загроз.

Начальник штабу армії США Джордж Кейсі визначив гібридну загрозу в 2008 році як противника, який включає «різноманітні та динамічні поєднання звичайних, нерегулярних, терористичних та кримінальних можливостей» [28].

Гібридні війни – це протистояння, що мають наступні ознаки:

- Гібридний супротивник використовує комбінацію стандартних та нестандартних методів. Гібридний супротивник також використовує підпільні дії, щоб уникнути приписування чи відплати. Методи використовуються одночасно в усьому спектрі конфліктів з єдиною стратегією.
- Гібридний супротивник гнучкий і швидко адаптується;
- Гібридний супротивник використовує передові системи озброєння та інші руйнуючі технології. Зараз таку зброю можна придбати за вигідними цінами. Більше того, нові технології адаптуються до поля бою, такі як стільникові мережі.
- Використання засобів масової комунікації для пропаганди. Зростання мереж масової комунікації пропонує потужні інструменти пропаганди. Використання підроблених веб-сайтів для поширення неправдивих історій є елементом гібридної війни;
- Гібридна війна відбувається на трьох окремих полях битв. Це звичайне поле бою, корінне населення зони конфлікту та міжнародне співтовариство [25].

У наш час ми стикаємось із низкою альтернативних визначень, а також рядом альтернативних концепцій, які можуть включати такі терміни як:

змішана війна, нелінійна війна, повстанська війна, війна 4-го покоління, постіндустріальна війна, асиметрична війна та війна нового покоління. У засобах масової інформації виступають такі вирази, як: війна хаосу, війна без правила, війна без лінії фронту, війна з безліччю пропагандистських напівправд та війна брехні, дипломатичний та економічний тиск, або війна, яка сприймається як концерт багатьох фортепіано.

Інформаційні війни, як елемент гібридної війни передбачають створення значної переваги в наступальних видах озброєнь, в знешкодженні систем захисту держави-супротивника засобами інформаційного впливу. Разом з гібридизацією засобів і шляхів ведення війн спостерігається зміна ключових політичних цілей, оскільки воєнні дії спрямовуються насамперед на дестабілізацію альянсів та окремих держав, для чого використовуються пропаганда, розбалансування, повстання, заморожені конфлікти «зі швидким розігрівом», тероризм, громадянські війни та інші внутрішні загрози, загострення політичних конфліктів і розширення внутрішніх ліній фронту для перевантаження організаційних потужностей держави і суспільства та зменшення можливостей застосування військових потуг.

Тобто, йдеться про те, щоб обмежити дієздатність урядів і парламентів як слабких країн у кризових регіонах, так і стійких демократичних держав, унеможливити гуманітарну інтервенцію або введення санкцій з боку західних держав. Тому спільним завданням альянсів, урядів, громадянського суспільства і військового сектору стає посилення власної стійкості до гібридних методів війни як передумови внутрішньо - і зовнішньополітичної дієздатності

Стаття, опублікована в «Global Security Review», «Що таке гібридна війна?», порівнює поняття гібридної війни з російською концепцією "нелінійної" війни, яку вона визначає як розгортання «звичайних та нерегулярних військових сил у поєднанні з психологічними, економічними, політичними та кібернападками». У цій праці частково приписуються труднощі з визначенням самого поняття війни «жорсткій» та статичній військовій класифікації, що використовується НАТО [37]. Крім того, для протидії

гібридній загрозі жорсткої сили часто буває недостатньо. Часто конфлікт розвивається під радаром, і навіть "швидка" реакція виявляється занадто пізньою. Переважаюча сила є недостатнім стримуючим фактором. Багато традиційних військових не мають гнучкості постійно змінювати тактику, пріоритети та цілі.

Гібридна війна не змінює характеру війни. Насильство залишається основним елементом цього виду війни. Її мета така ж, як і в будь-якого іншого акту війни, а саме, використовувати загрозу або використовувати організоване насильство для отримання фізичних або психологічних переваг над опонентом. Однак безліч термінології - гібридна, асиметрична, нетрадиційна, нелінійна, нове покоління, четверте і п'яте покоління, сірі війни тощо - відображає труднощі, які стратеги та вчені продовжують мати при категоризації складних збройних конфліктів двадцять першого століття. Хоча в даний час термін «гібрид» є найпопулярнішим, проте він далеко не єдиний, що описує ці війни.

Традиційним військовим шляхом складно реагувати на інформаційні війни. Організаціям колективної оборони, таким як НАТО, може бути важко домовитись про джерело конфлікту, що ускладнює відповідь.

Той факт, що багато збройних конфліктів стирає межі між війною та миром та передбачає використання інструментів, які традиційно не були частиною бойових дій, ще більше ускладнює проблему. Безсумнівно, для традиційних установ безпеки існує завдання вирішити широкий спектр загроз, визначених аналітиками та дослідниками гібридної війни. Якщо неправильно визначити дефініційну межу, то такий термін, як гібридна війна, стає надто всеохоплюючим, щоб мати якусь практичну користь для політиків. Визначте її дефініцію занадто вузько, і політики можуть не усвідомити значення багатьох нетрадиційних прийомів ведення війни, які використовуються противником як прелюдія або доповнення до застосування військової сили.

Незалежно від того, які з'являються загрози, стратеги повинні вирішити, як найкраще відбивати атаки, що застосовуються їхніми супротивниками, будь то державні чи недержавні суб'єкти. Іноді найкращі відповіді можуть передбачати

застосування конкретних політичних, інформаційних, економічних, дипломатичних або, у випадку фізичної загрози, військових інструментів державного апарату. Більш складні загрози вимагають комплексного підходу. Зазвичай найкращі стратегії передбачають координацію та керівництво всіма ефективними інструментами державної влади, незалежно від того, як визначається загроза.

Державна політика розробки передових технологічних, інформаційних та кібербезпекових систем стала однією з найважливіших складових національної безпеки у військовій сфері. Сучасні технології дають можливість впливати на сили ворога, створюючи потребу в реорганізації управління та захисту як від м'яких, так і від військових наслідків, у тому числі проведення спеціальної підготовка персоналу для підтримання бойової готовності.

Інформаційна війна доводить, що рівень національної безпеки та оборони повинен підтримуватися навіть в умовах світової економічної кризи і суттєво знижувати витрати на збройні сили. Розширення поля бою за межі кінетичних операцій та атак на інфраструктуру вимагає комплексного використання як традиційних сили, так і нового технологічного та синергетичного планування.

Практика військових конфліктів протягом останнього десятиліття свідчить про те, що стратегічна перевага дістається актору, який першим розуміє та впроваджує нові технології, який може використовувати їх як мультиплікатор сил, а отже має перевагу на своєму боці.

Командири повинні використовувати нові методи, хоча б лише для розуміння нових методів і доктрин, які може розгорнути ворог. Використання передових технологічних систем дає можливість підвищити ефективність вже існуючого державного військового потенціалу із меншими видатками, можливо, навіть на третину від традиційних бюджетів. Розглядаючи концепції національної безпеки та національних військових стратегій, уряди найбільш розвинених країн надають освіті та науці пріоритет як технологічно інтенсивним засобам бойових дій.

Сьогодні інформаційні технології всеохоплююче впливають на всі сфери життя сучасної людини. Розповсюдження інформації відбувається безперервно та дозволяє поглинати велику кількість новин щодня, в будь-якому місці, в будь-який час. Саме тому в сучасному світі важливо контролювати потік інформації, що проходить через споживача, а, що найважливіше, необхідно контролювати достовірність та безпечність тих даних, що потрапляють до користувача.

В умовах швидкого розвитку інформаційних технологій та все більшого використання сучасних гаджетів населенням різного віку, статі та соціального положення критично важливим стало запобігання поширення ворожого, неправдивого та пропагандистського контенту на території кожної окремої держави. Це питання набуває загальнодержавного значення на рівні з національною безпекою.

Найпоширеніші інструменти сьогоднішньої інформаційної війни - це фабрики тролів, боти та фейкові новини. Щоб вплинути на суспільство цільової країни, агресори поширюють маніпульовану або сфабриковану інформацію або навіть використовують поєднання обох цих видів.

Вони використовують автентичну інформацію таким чином, що породжує помилкові натяки. Однак інформаційна та кібервійна - це не лише маніпуляції. Це також нові технології, що використовуються для шпигунства та кібератак; отже, це створення неправдивої інформації, шантаж та лобіювання.

Активне використання ворожими силами методів інформаційного впливу на противника породжує виникнення феномена – «що більше ти знаєш, тим менше розумієш». Це пояснюється перерповненням інформаційного простору сфабрикованою або дискредитуючою інформацією, а отже, заважає звичайному користувачу самостійно розібратись в ситуації.

Інформаційна конфронтація між різними суспільними групами і державами ставить перед собою мету заволодіти ще більшим впливом на суспільство. Психологічну інформаційну війну починають як політичні партії та організації, так і терористи. Обидві ці групи ставлять перед собою мету

підкорити собі пізнання і особисту позицію людини, щоб він надалі зміг діяти всупереч своїм інтересам. Організації, що переслідують таку мету, впливають на свідомість людини за допомогою різноманітних маніпуляцій.

Для обробки свідомості використовують в малих кількостях правдиву інформацію, що при правильній розстановці створює цілу піраміду в істинно помилкової структурі. Таку конструкцію називають стратегічним міфом. Ця структура дозволяє при впровадженні замінити цілісне сприйняття на фрагментарне з помилковими і перекрученими поглядами. Імовірність того, що обман розкриється, існує, але на той час ця поведінка буде сприйматися суспільством як необхідна або вимушена.

Однак, незважаючи на подібний, досить докладний, розподіл на категорії, всі вони взаємопов'язані між собою і зазвичай в одній і тій же інформаційній війні може використовуватися відразу кілька форм інформаційного протиборства. Найефективнішою і небезпечною вважається психологічна форма дій, оскільки тут інформаційна війна спрямована на великі маси людей в свідомість і підсвідомість яких за допомогою спеціальних засобів здійснюється впровадження програмних і управлінських установок базової ідеології противника: людям нав'язують чужі їм цілі і роблять це так, що рядові громадяни були впевнені, що це саме їхня власна, рідна ідеологічна установка.

У боротьбі проти інформаційних загрози існують свої методи протидії, що дозволяють зменшити агресивний вплив на інформаційний простір. Відсутність інформаційного спротиву може мати негативний вплив на національну безпеку, а отже, важливо відстежувати та нівелювати ворожий інформаційний вплив.

Основні форми та методи протидії, що зазвичай використовуються для боротьби з інформаційними атаками:

- Бойкот експертною спільнотою та офіційними спікерами (політиками, чиновниками) медіа-сайтів опонента з метою деактуалізації вмісту;
- Формування бази даних ключових акторів ворога, блокування їх присутності на комунікаційних платформах (круглі столи, форуми, семінари тощо);

- Стигматизація професійної спільноти «агентів впливу», «корисних ідіотів» та інших суб'єктів;
- Створення організацій та центрів протидії інформаційній агресії, здатних чітко сформулювати фактичні загрози зовнішньому інформаційному впливу та визначити суб'єктів на основі перевірок та даних спецслужб.
- Дипломатичні санкції щодо суб'єктів (заборона на в'їзд).

Система протидії побудована в декількох горизонтах (особиста, інформаційна, внутрішня безпека, дипломатична) і являє собою сукупність «санкцій» та дій проти суб'єктів, які активно просувають в інформаційному просторі «руйнівний зміст»

Основні цілі, що переслідуються під час застосування методів протидії:

- Зміцнення довіри до державних та міжнародних інституцій;
- Підвищення обізнаності громадськості про цілі та вплив інформаційної агресії, структури та організації;
- Формування критичного підходу до інформаційних та соціальних установок, що забезпечують психологічну стабільність громадян щодо наслідків руйнівного змісту;
- Залучення великих мас людей до виробництва та просування «конструктивного» контенту;
- Сформувати систему активного впливу на основних діювих осіб та обмеження їх можливостей, участь у просуванні деструктивного змісту.

Реалізація цих методів протидії покладено на державу, як єдину інституцію, що здатна залучити приватний та державний сектор для захисту національних інтересів. Як відомо, саме захист національних інтересів являється однією з основних завдань будь-якої країни, що підтверджує тезу про те, що саме держава повинна нести відповідальність за формування комплексу протидії інформаційним загрозам.

РОЗДІЛ 2. ОСОБЛИВОСТІ ІНФОРМАЦІЙНОЇ ВІЙНИ РОСІЇ ПРОТИ УКРАЇНИ

Якщо в минулому столітті війна проводилася за допомогою зброї: танків, автоматів і ракет, то в ХХІ інформаційно-інтелектуальному столітті головною зброєю є «незалежні» експерти та журналісти, які стріляли на ураження за допомогою засобів масової інформації під впливом світової політичної еліти. Ця інформаційна війна почалася з переходом в інформаційну еру. Одним з найпереконливіших прикладів є конфлікт між Росією та Україною, що розпочався у 2014-2015 рр. з фактичної присутності російських військових сил в Донбасі, і який досі залишається невирішеним. Українські ЗМІ стверджують, що російські війська брали і беруть участь у військових діях на Україні, російські – ні.

Агресія Росії проти України постійно супроводжується інформаційною кампанією, яка має ті ж характерні особливості, що і війна. Насправді інформацією можна атакувати, зробити обманний маневр або повністю підмінити інформаційний потік.

Засоби масової інформації різних країн суперечливо висвітлювали події на Україні. Більшість з них звинувачують Російську Федерацію на початку військових дій і приписують їй участь в громадянській війні шляхом введення російських військ на територію Донбасу.

Росія розпочала свою добре сплановану збройну агресію проти України 20 лютого 2014 року, здійснивши військову операцію своїх Збройних сил щодо захоплення частини української території – Кримського півострова. Цю дату навіть не заперечує Міністерство оборони Росії, як це зазначено на відомчій медалі «За повернення Криму». Фактично, лише наступного дня Віктор Янукович втік з Києва; і вже 22 лютого 2014 року Верховна Рада України прийняла Постанову «Про відмежування Президента України від виконання конституційних повноважень та призначення дострокових президентських

виборів в Україні», використана Росією як привід для звинувачень у нібито «неконституційний переворот в Україні».

Військова агресія - лише один з елементів російської гібридної війни проти України. Інші елементи охоплюють:

- пропаганда, заснована на брехні та фальсифікаціях;
- торгово-економічний тиск;
- енергетична блокада;
- терор та залякування українських громадян;
- кібератаки;
- рішуче заперечення самого факту війни проти України, попри велику кількість незаперечних доказів;
- використання проросійських сил та держав-сателітів у власних інтересах;
- звинувачення іншої сторони у власних злочинах.

Росія використовує передову форму гібридної війни в Україні з початку 2014 року, яка значно спирається на елемент інформаційної війни, який росіяни називають «рефлексивним контролем» [33]. Рефлексивний контроль змушує сильнішого супротивника добровільно обирати дії, найбільш вигідні для російських цілей, рішуче формуючи сприйняття супротивника ситуації.

Ключовими елементами російських рефлексивних методів управління в Україні були:

- Операції заперечення та обману з метою приховування або затуманення присутності російських сил в Україні, включаючи відправлення «маленьких зелених чоловічків» у формі без знаків відмінності;
- Приховування цілей і завдань Москви у конфлікті, що сіє страх в одних, а іншим дозволяє переконати себе, що цілі Кремля є обмеженими та зрештою прийнятними;
- Збереження поверхнево вірогідної законності для дій Росії, заперечуючи причетність Москви до конфлікту, вимагаючи від міжнародної

спільноти визнати Росію зацікавленою силою, а не стороною конфлікту, і вказуючи на нібито рівноцінні західні дії, такі як одностороннє проголошення незалежності Косово у 1990-х та вторгнення в Ірак у 2003;

- Одночасне погрожування Заходу військовою силою у вигляді перельоту повітряного простору країн НАТО та країн, що не входять до НАТО, погроз використання російської ядерної зброї та перебільшених заяв про військову доблесть та успіх Росії;

- Розгортання великих та складних глобальних зусиль для формування розповіді про український конфлікт за допомогою офіційних та соціальних медіа.

Результати цих зусиль неоднозначні. Росія утримала Захід від матеріального втручання в Україну, дозволивши собі час побудувати та розширити власну військову участь у конфлікті. Це посіяло розбіжності в альянсі НАТО і створило напруженість між потенційними супротивниками щодо того, як відповідати. Однак це принципово не змінило народних або елітних поглядів на дії Росії в Україні, а також не створило інформаційного середовища, сприятливого для Москви.

Володимир Лефевр, один з головних радянських учених, що вивчав рефлексивний контроль, писав, що "приймаючи своє рішення супротивник використовує інформацію про зону конфлікту, про його власні та наші військові дії, про їх здатність до бою тощо. Ми можемо впливати на свої канали інформації та надсилати повідомлення, які зміщують потік інформації у спосіб, сприятливий для нас. Суперник використовує найсучасніші методи оптимізації та знаходить оптимальне рішення. Однак це буде не бути справжнім оптимальним рішенням, а рішенням, визначеним нами [26].

Перш за все, Росія досі не змогла перетворити грандіозні переваги своєї стратегії гібридної війни на великі та стійкі успіхи на місцях в Україні. Крім того, схоже, Москва може досягти точки зменшення віддачі, продовжуючи стратегію, яка частково покладається на її несподіваність в Україні. Проте та

сама доктрина рефлексивного контролю зуміла здивувати Захід у Сирії. Таким чином, Захід повинен пробудити себе до цієї стратегії та її адаптації.

Однією з відмінних рис «гібридної війни» в Україні є те, наскільки вона зайняла всі аспекти соціального життя, наскільки широкомасштабна, багатовимірна та використовує багатофакторну інформацію, орієнтовану як на психологічні, так і на кібернетичні джерела. Хорошим прикладом такої діяльності є інноваційні та високотехнічні зразки зброї та військової техніки, застосовані під час анексії Криму 2014 року, а також бойові дії на сході України з 2014 року.

Розглянемо російські ЗМІ, що приймали участь в інформаційній війні у один з моментів найбільшої конфронтації конфлікту між Україною та Росією – початок 2014 – кінець 2015 рр. Цей період відзначається анексією Кримського півострову Росією та початком ведення бойових дій в Донецькій та Луганській областях. На цьому прикладі буде зрозуміло як Російській Федерації вдається виправдовувати в інформаційному полі навіть такі кричущі насильницькі дії проти іншої держави.

Вибіркову сукупність для аналізу російських ЗМІ складали:

- федеральні газети: «Аргументы и факты», «Московский Комсомолец» та «Коммерсант»;
- інформаційні агенції: «РИА Новости», «Lenta.ru»;
- Інтернет-сторінки, адреси яких вказані в результатах Google-пошуку (тільки російською мовою, тільки в Росії) за запитами «война в Украине», «российские войска в Украине», «российские войска в Донбассе», «российско-украинский конфликт».

Вибіркову сукупність для українських ЗМІ склали:

- Українська правда;
- Дело (розділ: Війна з Росією);
- УНІАН;

- Українські національні новини, а також веб-сайти, знайдені за допомогою пошукової системи Google.

Під час дослідження було опрацьовано статті періодичних та інтернет видань за вибраний період часу, що є у наявності в мережі Інтернет. Публікації відбирались за наявністю в тексті ключових слів: «война в Украине», «российские войска в Украине», «российские войска в Донбассе», «российско-украинский конфликт» - для російських ЗМІ; та: «Війна в Україні», «російські війська в Україні», «російські війська в Донбасі», «російсько-український конфлікт», «Війна на сході України», «Окуповані території» - для українських ЗМІ.

Таким чином, були розглянуті причини війни, які визначають російські джерела ЗМІ. У таблиці 1 викладено найчастіше уживані. Для складення таблиці було проаналізовано вибірккову сукупність російських видань за 2014-2015 рр.

Таблиця 1. – Причини війни в Україні з точки зору російських ЗМІ.

Джерело	Причина війни
«Аргументы и факты»	величезна корупція; вибірковість судової системи; слабка система захисту власності; кримінально-політичне рейдерство; офшоризація; жадібність та егоїзм еліти; розподіл спільноти на бідних та багатих.
«Московский Комсомолец»	тиск США на українську владу.
«Коммерсант»	поклади сланцевого газу в регіоні, де збройне протистояння носить найзапекліший характер – між Луганськом, Слов'янськом та Краматорськом.
«РИА Новости»	непрофесіональні дії Заходу;

	геноцид російсько-українського народу.
«Lenta.ru»	державний переворот, що підтримується американськими та європейськими партнерами; чітко розроблені та спрямовані дії США.
Інші інтернет-видання, що висвітлювали інформацію за даною темою.	недостатня освіченість громадян України; підтримка значимості американського долара в якості світової валюти; підрив довіри до Росії, шляхом втягнення її у конфлікт; тиск українських націоналістів на людей, що прихильні до російської культури; використання України в якості «приманки» для Росії; рішення української влади призупинити процес підписання договору про асоціацію з ЄС.

На основі проведеного аналізу можна зробити висновок, що російські ЗМІ не виділяють якоїсь конкретної причини виникнення конфлікту на території України, і водночас яскраво використовують різні прийоми інформаційного протиборства. Кожне джерело по-своєму описує причини конфлікту, в залежності від специфіки та стилю викладення інформації видання.

Розглянемо основні прийоми, що використовуються російськими засобами масової інформації для ведення інформаційної конфронтації:

1. Пряме спростування – найбільш поширений прийом ведення війни зі сторони Росії. Президент України, прем'єр-міністр, секретар РНБО, Президент США, посол США в Україні та ін. не раз робили гучні заяви про присутність російських військ та використання російської зброї на окупованих територіях. Російські ЗМІ публікують гучні заяви іноземних осіб що саме Росія вважається агресором і бере участь у війні в Україні. В кінці цих заяв робиться спростування про те, що «міжнародними спостерігачами жодного разу не було помічено присутності російських військових на території Донбасу.

2. «Навішування ярликів» – namecalling. Російські ЗМІ публікують інформацію про те, що Сполучені Штати ведуть війну проти Росії, діючи через третю сторону – Україну. США навмисно надають партнерам по НАТО неправдиву розвідувальну інформацію, на основі якої ті заявляють про присутність російських військ на Україні. Відносно України, російські ЗМІ використовують образливі прізвиська, такі як «фашисти», «нацисти», «бандерівці», «маріонетки Заходу», «бандити», «мафія», та ін.

3. «Посилання на авторитет». Російські ЗМІ посиляються на впливових особистостей у Росії та висвітлюють їх заяви, щодо війни на Донбасі як істину в останній інстанції. Це, наприклад, заяви В.В.Путіна: «В Україні російських військ немає. Ми не беремо участі в громадянській війні в Донбасі»; також це заяви Д. Медведєва, Д. Пєскова та ін. Такі посилення на перших осіб держави додають важливості заяві та змушують, у поєднанні з іншими прийомами інформаційного протистояння, повірити у сказане.

Таким чином, можна прослідкувати тенденцію впливу висловлювань впливових політиків та інших людей викликають позитивну або негативну реакцію у категорії людей, на яких спрямовується маніпулятивний вплив. Такі висловлювання, як правило, носять оцінювальні судження щодо людей, подій і висловлюють їх схвалення або засудження. Таким чином, встановлюється зворотний зв'язок з населенням за допомогою ЗМІ.

4. «Блискуче узагальнення». Це стосується інформації про регулярні гуманітарні допомоги Україні зі сторони Росії. На думку російських ЗМІ гуманітарні допомоги Україні допомагають підняти загальний патріотизм країни та посилити єдність колишнього радянського народу в головах пересічних російських громадян.

5. «Перетасовка» фактів. Під час вибору інформації до публікування у свої виданнях, російські ЗМІ ретельно вивчають та відбирають інформацію. Російські ЗМІ, на відміну від українських, не публікують інформацію про докази участі РФ у військових діях в Донбасі. Таким чином, основна мета даного прийому в інформаційній війні - сформувати думку російських

громадян про те, що Росія не причетна до конфлікту на Україні, який стався через помилки внутрішньої політики країни, що проводиться під впливом Заходу.

6. Захоплення медіапростору. Російська владна верхівка ретельно фільтрує всю інформацію, що публікується в засобах масової інформації. Таким чином, в голови пересічних російських громадян потрапляє лише те, що вважає за потрібне владна еліта країни. За словами деяких телеведучих, вони не можуть запрошувати на свої телепередачі людей, що цікавили б звичайних людей, якщо їхня офіційна позиція щодо чинної влади не дружелюбна.

7. Переписування історії. Це прийом, що використовує Росія вже давно і не лише у сфері ЗМІ. Так, в нових підручниках по історії, що були випущені 2015 року та використовуються учнями з цього ж року, повністю виключено поняття «татаро-монгольського ярма». Замість цього йдеться про залежність руських земель від ординських ханів.

Якщо досліджувати співвідношення використання прийомів у російських засобах масової інформації, то ми бачимо, що найпоширенішими прийомами є «Пряме спростування», «Навішування ярликів», «Посилання на авторитет» та «Перетасовка фактів».

Інформаційна війна путінської Росії проти України призвела до того, що більше половини опитаних росіян готові воювати з українцями. Вірусом ненависті особливо заражені молоді люди, які ніколи не були в Україні і не мають контактів з її громадянами. Старших людей лякають «бандерівцями-головорізами, які прийшли до влади». Це результат планомірної тотальної брехні, яка розробляється ідеологами Кремля, транслюється телебаченням і поширюється усіма можливими шляхами [9].

Використовуючи засоби масової інформації російський уряд зміг виправдати агресію в Криму та на сході України в очах свої громадян настільки, що більшість людей не тільки підтримують це, а й відчують особисту неприязнь та агресію по відношенню до українців.

Українських громадян виставляють неосвіченими, такими, що не знають власної історії та просто не розуміють, що Росія хоче їх врятувати від Заходу, який посягає на українські землі та сільське господарство [9]. Дезінформація, що проводиться російськими ЗМІ має на меті створити навколо України імідж «маріонеткової», підконтрольної Заходу країни.

Одним з найважливіших та найдієвіших прийомів для виправдання введення російських військ на територію України є право націй на самовизначення. Саме цим найчастіше аргументує Кремль захоплення Криму. Офіційна версія стверджує, що громадяни Криму самоорганізувалися в збройні угруповання та самі провели референдум щодо вступу до Російської Федерації, а Кремль всього лише підтримав народ та протягнув «руку допомоги», щоб врятувати російськомовне населення півострова від «бандерівців», які ненавидять російську мову та Росію [9].

Така сама ситуація відбулася, на думку Кремля, в східних областях України: зважаючи на жахливі умови життя Луганська та Донецька області вирішили відділитися від України та приєднатися до складу РФ, але українська армія силою намагається втримати їх в складі країни [9].

Західні спостерігачі після анексії Криму та вторгнення в східну частину України часто сприймають гібридну війну як сучасну модель ведення військової діяльності Російською Федерацією та попереджають, що вона може бути використана проти колишніх республік СРСР, та навіть Польща [29].

За словами генерала Філіпа Брідлава: "Росія веде найдивовижніший бліцкриг з питань інформаційної війни, який ми коли-небудь бачили в історії інформаційної війни" [40].

Отже, інформаційну кампанію Кремля можна розбити на наступні етапи:

1. Початок 1990-х - липень 2013 року - підготовча фаза, або інформаційне зондування ситуації» (проведення точкових інформаційних заходів в економічній, військовій, інформаційній, політичній та інших сферах діяльності Української держави, які не створювали загроз національній безпеці України).

З цього приводу потрібно згадати риторику, яка формувалася в 1992 році:

- віце-президент РФ О. Руцькой: «Крим - це частина Росії» [24];
- мер Санкт-Петербурга А. Собчак: «Крим ніколи не належав Україні»[4];
- голова Верховної Ради РФ Р. Хасбулатов: «Чорноморський флот колишнього СРСР буде належати Росії» [4];

В результаті в червні 1993 року на військових базах Криму 203 військових корабля (це 80 відсотків) підняли російський прапор. Все відбувалося під виглядом стихійної ініціативи суднових команд. Згодом ця акція стала основою для створення Чорноморського флоту РФ. Це була, по суті, перша російська інформаційна диверсійна атака з метою змусити Україну сформувати російський військово-морський компонент на Чорному морі. Паралельно з цим Росія чинила тиск на українське керівництво щодо вилучення в Україні ядерної зброї і підписання нею гучного Будапештського меморандуму.

Середина 90-х років характеризувалася рідкісними поодинокими заявами російських політиків про нібито «російське походження» Севастополя.

У 2015 році Л. М. Кравчук повідомляв, як Росія намагалася порушити територіальну цілісність України 1992 року. «Україна в рамках своєї територіальної цілісності прийняла рішення, що всі війська, які знаходяться на території України, повинні бути підпорядковані Україні. І я видав указ про підпорядкування Чорноморського флоту України. У той же день Єльцин видав свій указ про підпорядкування Чорноморського флоту на території України Росії. Це вже був перший крок територіального втручання. Почалися дуже складні процеси. Деякі кораблі з Севастополя взяли курс на Одесу. По них відкрили стрільбу бойовими снарядами. Цього ніхто не знає, але це було і це в історії зафіксовано» пригадує Л. М. Кравчук [18].

З кінця 1990-х в інформаційному полі України спостерігалися активні заходи зовнішнього інформаційного впливу. В Україні вони були зафіксовані як інформаційні операції (під умовними назвами) «газова війна», «блокування розвитку авіаційної галузі», «мовна проблематика», «Чорноморський флот в

Криму», «маякового війна», «сирна війна», «трубна війна », «цукеркова війна» та ін.

Крім того, відмінною рисою того часу було створення в Україні десятків проросійських громадських організацій: різноманітних об'єднань росіян, товариств російської історії і культури, національно-патріотичних організацій. Практично всі організації отримували фінансування з фондів, афілійованих з Кремлем і Міністерством закордонних справ Росії. Їх активна діяльність спостерігалася в південних областях, на сході України, рідше в центральній частині країни та менше на заході.

Особливу роль в плані інформаційного тиску Росії на Україну зіграв конфлікт 2003 року щодо острова Тузла. Він мав зондований характер в плані можливого використання фактора відсутності в Україні Державного кордону. Після розпаду СРСР кордон з Росією не було делімітовано і демарковано. Москва всіляко обходила це питання, посиляючись на договір 1997 року «Про дружбу, співробітництво і партнерство між Україною і РФ».

Окремо слід згадати часті візити до Криму представників російської Держдуми В. Жириновського, Г. Зюганова або мера Москви Ю. Лужкова та ін. Їх зустрічі з моряками ЧФ РФ, членами проросійських організацій і ветеранами мали пропагандистський характер. Вони підтримували ЧФ РФ будівництвом житла, клубів для російських військових, поширювали літературу та організовували концерти під проросійські гасла типу «Крим – це Росія».

Починаючи з 2010 року інформаційна ситуація в Україні стала більш схильна до російського вектора. Президентом України став Віктор Янукович, який за короткий час створив систему авторитаризму і російської «керованої демократії». Через два місяці після свого обрання Янукович підписує з Росією Харківські угоди, згідно з якими перебування ЧФ РФ в Криму було продовжено на 25 років за знижки на покупку російського газу. Після цього в українських медіа стало з'являтися більше матеріалів про переваги Митного союзу з Росією.

2. Серпень – листопад 2013 року – фаза «створення інформаційного плацдарму» в Україні.

Під час свого візиту до Києва, присвяченого святкуванню 1025-річчя хрещення Русі, Путін у своїй промові дав зрозуміти, що Росія не збирається відпускати від себе Україну. А вже у вересні 2013 року російський президент призначив своїм радником Владислава Суркова. На новій посаді Суркову було доручено відповідати за роботу з громадською думкою в Україні.

Як наслідок, за чотири місяці в інформаційному просторі України підвищився градус інформаційної активності Кремля і зазначалося створення трендів інформаційного впливу:

- корупція в політичному керівництві України;
- нежиттєздатність української економіки;
- наявність факторів розшарування українського суспільства;
- зростання невдоволення народу щодо керівництва України та ін.

Паралельно з цим в Україні відзначалася активізація діяльності проросійських громадських рухів, ЗМІ, електронних ресурсів.

У Криму, особливо в м. Севастополі, посилено формувалася російська ідеологічна платформа: активізувалися благодійні, культурні фонди, відкривалися інформаційно-просвітницькі центри, створювалися нові громадські організації проросійської спрямованості. Їх робота була спрямована на об'єднання навколо проросійських ідей якомога більшої аудиторії.

3. Грудень 2013 - лютий 2014 року - фаза «інформаційної агресії» в Криму і «розгойдування ситуації» на Донбасі. Її характерні риси:

- сплеск антиукраїнської риторики;
- інформаційна блокада регіонів конфлікту;
- залучення масової аудиторії в саботаж діючої влади;
- різка активізація проросійських громадських і націонал-патріотичних організацій;
- демонстрація організованою воєнізованою силою;

- надання тиску на місцеві органи влади;
- блокування діяльності органів виконавчої влади та ін.

До основних інструментів інформаційного впливу Кремля в цей період на аудиторію України можна віднести:

- відкриті заклики російських політиків і громадських діячів до відокремлення Криму і Донбасу від України (К. Затулін, В. Жириновський, Ю. Лужков, Г. Зюганов і ін.);
- посилення в соціальних мережах «ВКонтакте», «Однокласники», «Мій світ» та ін. Пропаганди щодо відділення областей південної і східної частин України і переходу їх під протекторат Росії;
- поява закликів до «російських патріотів» підтримати розкол України і попрямувати в українські міста для «надання допомоги» антиукраїнським силам в соціальних мережах, блогах, на телевізійних ток-шоу;
- виникнення хвилі закликів від російських волонтерських організацій націонал-патріотичного спрямування до «збору коштів для допомоги росіянам в Україні»;
- формування сепаратистських думок щодо України через російські релігійні об'єднання, центри астрологів, освітні установи та ін.

4. Березень - червень 2014 року - фаза «широкомасштабного інформаційного пресингу» - проведення серії інформаційних кампаній, які забезпечують анексію Криму і вторгнення проросійських воєнізованих формувань на Донбас.

Метою цих кампаній було нав'язування вигідною кремлівської позиції по відволіканню уваги аудиторії від факту військової окупації Криму в сторону розпалюваних подій на сході України. Характерна ознака цієї фази - масове використання інформаційного ресурсу Кремля і насичення своїм контентом українського інформаційного потоку. При цьому російські медіа мали намір витіснити українські ЗМІ з схеми поточного інформування.

18 березня 2014 року Росія заявила про приєднання Криму. З цього часу інформаційна кампанія Кремля на окупованому півострові переключилася на популяризацію ідеології «Русского мира». Це досягалося методами агітації (масової інформації та інтернет-ресурси) і введення елементів цензури (спецоргани).

5. Липень 2014 - січень 2015 року - фаза «закріплення інформаційного домінування» в ситуації на Донбасі виникала в стилі традиційного набору класичних інформаційних заходів, які до цього були вже Грузії, Югославії, Іраку і Афганістані.

Для цього періоду найбільш характерні такі гучні інформаційні операції:

- «Гуманітарна катастрофа» в регіонах України полягала в створенні щільного інформаційного потоку негативної інформації;
- Спецоперація «Гуманітарний конвой», крім імітації доставки продовольства і медикаментів в постраждалі регіони, мала на меті таємно вивезти тіла загиблих бойовиків і евакуювати тяжкопоранених в Росію;
- «Забалакування теми збитого терористами "Боїнга"» направлено на спотворення реального змісту факту злочину, вчиненого російськими терористами. В результаті цієї операції розслідування злочину досі не закінчено, а винні не покарані;
- «Замовчування участі російських солдатів у війні проти України» - це довгострокова операція, метою якої є повне заперечення причетності Росії до військових дій на Донбасі і заявки, що цього немає ніяких доказів. Надані свідчення присутності на Донбасі російських військ всіляко висміювалися і спростовувалися;
- «Зрив мобілізації в Україні» проводилося з метою нав'язати думку про марність і ущербності призову військовозобов'язаних для створення резерву сил АТО і ін. В цьому сенсі показовим став мем українською мовою, який копіював поширені написи на сигаретних пачках - «Мобілізація вбиває!».

6. Лютий - серпень 2015 року - фаза «стабілізації інформаційної ситуації».

Стабілізація інформаційної ситуації має на увазі недопущення падіння досягнутого рівня інформаційної присутності в інформаційному потоці.

Прогресивна частина інформаційної кампанії Росії фактично завершена. Завданням цього етапу є пошук шляхів, що дозволяють утримати інформаційну ситуацію на певному рівні.

7. Вересень 2015 року - по теперішній час - фаза «інформаційної адаптації», головною метою якої є створення умов для сприйняття населенням склалася в окупованому регіоні ситуації в необхідному ключі.

Суть в тому, що в невизнаних республіках існують групи людей, які не приймають позицію російських терористів, але висловити відкрито свою думку не можуть через загрозу їхньому життю. Завдання цього етапу - нівелювання таких груп шляхом формування у всього населення довіри до проросійських представникам влади і їх засобам масової інформації.

Інформаційна адаптація практично виключає інформаційний тиск як метод. У цьому випадку застосовуються прийоми роз'яснення і переконання.

Загальні характеристики етапу «інформаційної адаптації»:

- збереження медійного домінування Росії в тимчасово окупованих регіонах України;
- «консервація» каналів інформаційного впливу на аудиторію України;
- проведення спеціальних інформаційних заходів в окупованих регіонах;
- подальше просування проросійської ідеології;
- «показове» виконання положень Мінських домовленостей;
- демонстрація «демократичною влади» в окупованих регіонах нібито без участі в цьому процесі Кремля;

Одним з методів досягнення «інформаційної адаптації» в окупованих регіонах Донбасу є створення системи контролю над медійним потоком. Цей принцип реалізований режимами «народних республік», що дозволяє

використовувати засоби інформації і комунікації в інтересах встановленої там диктатури.

Крім усього, важливою особливістю нової фази є різке зниження обсягу інформаційних повідомлень про Україну. Якщо в період «інформаційного пресингу» українська тематика займала понад 90 відсотків всього інформаційного потоку, а в фазі «стабілізації інформаційної ситуації» цей показник досягав рівня 25-45 відсотків, то в період «інформаційної адаптації» Україні відводиться всього 5-8 відсотків інформації. Вивільнилися інформаційний потік Кремль швидко заповнив сирійської проблематикою - інформуванням про проведення російською авіацією бомбардувань в Сирії.

Російська інформаційна війна не є загрозою, ізольованою для Європи та США, скоріше це глобальна стратегія, яка впливає на кожен регіон світу в різній мірі в силу своїх великих розмірів, маси та складності. Російський підхід до інформаційної війни є цілісним і включає як кібератаки, так і інформаційні операції як цілісні елементи, які працюють у тандемі для досягнення цілей російської зовнішньої політики. Крім того, російський підхід має на меті підірвати не тільки збройні сили супротивника, але й впливати на сприйняття цільового населення таким чином, що сприяє російським інтересам.

Якщо звернутися до першопричин конфлікту між Україною та Росією, видається очевидним факт про глибоке підґрунтя конфлікту та його неминучість. С. Гантінгтон у своїй праці «Зіткнення цивілізацій» стверджував, що у світі існує дев'ять цивілізацій, між якими існують «лінії розломів» - так звані кордони, що розділяють цивілізації на історичному, економічному, соціально-політичному та інших рівнях. (Зіткнення цивілізацій, Сэмюэл Филлипс Хантингтон) На цих «лініях розлому» і можливий конфлікт, як вважає автор. І саме на такій «лінії розлому» знаходиться Україна. Він вказував, що ця лінія проходить просто по центру України і розділяє її на Схід, що тяжіє до Росії, та Захід – до Європи.

Також Гантінгтон вказував, що через Крим може статися розкол України, а також, що можливим є варіант, де східна частина України відійде до Росії, а

початком цього «розколу» стане Кримський півострів. Очевидно, що певні закономірності вже існуючого конфлікту простежувалися вже давно і навіть передбачалися варіанти подій.

Не можна заперечувати, що Гантінгтон був правий, коли описував розкол України на Схід та Захід, адже цей факт не залишає сумнівів – відмінності присутні. Для збереження цілісності країни необхідно усвідомити та прийняти факт культурної, мовної, національної та інших різноманітностей українців, усвідомити спільні прагнення до збереження єдності країни, та разом рухатися до спільного майбутнього. Лише в єдності можливо подолати спільного ворога та вийти переможцем з такої гри, і «інформаційної» зокрема.

На закінчення можна сказати, що «інформаційна війна» як один із компонентів гібридної війни, яку Росія веде проти України, не була абсолютно новим явищем у постмайданівський період в Україні. Іншими словами, інформаційна війна до дестабілізації території Донбасу проходила в межах України. Отже, процес сприяв поляризації Сходу та Заходу України, що відтворювало міфи про ексклюзивність Донбасу. У цьому сенсі як національні, так і місцеві ЗМІ разом із політиками та елітами зіграли "досить добре", щоб посилити або пришвидшити ізоляцію людей Донбасу від решти України. З одного боку, місцеві ЗМІ регіону Донбасу використовували такі терміни, як «фашисти», «нацисти» або «маріонетки Заходу», які форсують політику українізації на Донбасі. З іншого боку, ЗМІ на Заході України описували Донбас як «бандитів», «мафію» або «московських маріонеток». Зрештою, обидві сторони не зробили нічого кращого, як взаємно сприяли ізоляції регіону.

У результаті проаналізувавши, як Росія веде інформаційну війну проти України, можна зробити деякі висновки. По-перше, вона показала, що підтримані Кремлем російські ЗМІ відіграли критичну роль в інформаційній війні. Інформаційні канали та газети, такі як «Аргументи и факти», «Коммерсант», «Московский комсомолец», «РИА Новости» є одними з інших інформаційних засобів Росії. Крім того, Москва також ефективно використовує соціальні мережі для управління сприйняттям громадськості або дискредитації

України. Росія почала вирощувати свою «армію тролів», особливо після події Євромайдану, щоб виправдати як анексію Криму, так і участь на Донбасі, хоча Москва офіційно заперечує свою участь у війні. Однак, такі поняття, як «фашисти», «нацисти», «бандерівці», «маріонетки Заходу», «бандити», «мафія», та ін., були поширеними до і після конфлікту на Донбасі. Основна відмінність між цими двома періодами полягає в тому, що перша частина відбулася в Україні та закріпила ці концепції, тоді як друга - між Україною та Росією. Таким чином, стає зрозуміло, що риторика, яку переважно використовували російські ЗМІ під час конфлікту на Донбасі, була фактично сформована до початку конфлікту.

До кібератак слід ставитись дуже серйозно, а держава повинна інвестувати в наукові дослідження та розробку спеціалізованого програмного та апаратного забезпечення, здатного вести боротьбу в галузі кібербезпеки. Тим часом військові та цивільні фахівці повинні отримувати постійну освіту та навчання з кібербезпеки. Веб-сайти, електронні листи та внутрішні мережі стратегічних установ повинні бути добре захищені шляхом встановлення найкращого антивірусного програмного забезпечення. Працівники повинні бути навчені розпізнавати та уникати можливих загроз. Існування команд для участі в контрреволюційній боротьбі з повстанцями може зробити вирішальний внесок у боротьбу з гібридними загрозами. І останнє, але не менш важливе: існування антипропагандистського агентства для підвищення обізнаності про фальшиві новини є обов'язковим для протидії гібридній війні.

РОЗДІЛ 3. ПРОТИДІЯ ІНФОРМАЦІЙНІЙ АГРЕСІЇ: УКРАЇНСЬКИЙ ВИМІР

Попри гібридну агресію Росії проти України, що триває уже кілька років, система державної безпеки все ще має прогалини, які заважають їй відновити територіальну цілісність та суверенітет та виконувати свої зобов'язання щодо забезпечення безпеки українського суспільства. Як наслідок, страждають громадяни України, які проживають в окупованому Криму та ОРДЛО, «сірих» зонах та прилеглих до лінії конфронтації областях України, інших областях України, які безпосередньо зазнають впливу агресора чи гібридних загроз.

Основним положенням Конституції України (Закон від 28.06.1996 № 254к / 96-ВР) у цій галузі є стаття 17, яка говорить: «Захист суверенітету та територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою цілої української нації».

Можна знайти деякі відповіді в Законі «Про інформацію» (Закон від 02.10.1992 № 2657-XII), який регулює відносини, пов'язані з інформацією, основні аспекти державної політики, право на інформацію, її гарантії, встановлює види інформації тощо. Однак закон мовчить про визначення інформаційної безпеки та її зв'язок із кібербезпекою.

Набагато кориснішим джерелом нормативного забезпечення є Закон "Про основи національної безпеки України" (Закон від 19.06.2003 № 964-IV). Стаття 7 визначає дев'ять основних напрямків загрози національним інтересам та національній безпеці України. Вони є сферами зовнішньої політики, державної безпеки, військової та прикордонної безпеки, внутрішньої політики, економіки, соціальної та гуманітарної, науки та техніки, цивільної оборони, інформації.

27 січня 2016 року в Україні було видано указ Президента України про рішення Ради Національної безпеки та оборони «Про стратегію кібербезпеки України» [12]. Мета цього документу – створити необхідні умови для безпечного кіберпростору та його використання в інтересах людей, суспільства та влади.

Рада національної безпеки та оборони визначила наступні цілі для досягнення основної мети:

- 1) Створення національної системи кібербезпеки;
- 2) Посилення спроможності зацікавлених сторін у кібербезпеці протидіяти військовим кіберзагрозам, кібершпигунству, кібертероризму та кіберзлочинності, з метою поглиблення міжнародного співробітництва щодо кібербезпеки;
- 3) Забезпечення кібербезпеки державних електронних та інформаційних систем та інформаційної інфраструктури під юрисдикцією України.

Рада національної безпеки та оборони визнає важливість кіберпростору та його вразливість до зовнішнього впливу. Це підкреслює особливу серйозність кібербезпеки для військової сфери, де використання сучасних інформаційних технологій значно зросло завдяки гібридній війні з Росією.

Також схвалюється думка про те, що державні об'єкти можуть бути об'єктами кібертероризму, та що інформаційні ресурси фінансових установ, транспортних та енергетичних компаній, державних агентств відповідальні за реагування на надзвичайні ситуації часто стають об'єктом кібератак та кіберзлочинів.

Такі вразливості перетворюються на кіберзагрози через:

- Недостатню інфраструктуру електронного зв'язку, її розвиток та захист у порівнянні із сучасними вимогами;
- Недостатній та непослідовний захист кібероб'єктів;
- Недостатній розвиток організаційно-технічної інфраструктури для забезпечення кібербезпеки та кіберзахисту державних електронних інформаційних ресурсів;
- Недостатня спроможність зацікавлених сторін у сфері безпеки та оборони протидіяти кіберзагрозам військового, злочинного та терористичного характеру;
- Недостатня координація та співробітництво між органами, що займаються кібербезпекою.

Законодавство України з кібербезпеки базується на принципах поваги прав і свобод громадян, поваги до людської гідності, захист інтересів людей, суспільства та держави, забезпечення суверенітету та територіальної цілісності України. Основними завданнями кібербезпекової стратегії є – захист українського суспільства від агресивного впливу руйнівної пропаганди, особливо тієї, що здійснюється Російською Федерацією; захист українського суспільства від агресивного інформаційного впливу Російської Федерації, спрямованого на пропаганду війни, розпалювання міжнаціональної та релігійної ворожнечі, загарбницьку зміну конституційного ладу або будь-яке порушення суверенітету або територіальної цілісності України; розвиток медіакультури суспільства та соціально відповідального медіа-середовища; створення систем та механізмів захисту від негативних зовнішніх інформаційних та психологічних впливів, особливо пропаганди, на основі положень міжнародного права; створення позитивного іміджу України у світі, надання швидкої, точної та об'єктивної інформації міжнародній спільноті про події в Україні; побудова системи іноземного мовлення України та забезпечення доступності іноземного українського каналу в кабельних мережах та в супутниковому мовленні за межами України.

В останні роки Україна прийняла низку актів, що регулюють питання кібербезпеки, які становлять її національну правову базу щодо кібербезпеки:

- Прийнята у 2016 році Національна стратегія кібербезпеки України є актом підзаконного законодавства, який визначає цілі та пріоритети кібербезпеки до 2021 року.
- Закон про кібербезпеку є доволі рамковим набором правил та вимог на високому рівні; він не вдається в деталі, залишаючи це для вирішення вторинного законодавства, яке має бути затверджено Кабінетом Міністрів України.

Загрозами, пов'язаними зі сферою інформаційної безпеки, переліченими в законі, є:

- обмеження свободи слова та доступу до публічної інформації;

- поширення культу насильства, жорстокості та порнографії засобами масової інформації;
- маніпулювання суспільною совістю (наприклад, шляхом поширення неправдивої, неповної чи упередженої інформації);
- розголошення державної таємниці або іншої інформації з обмеженим доступом, яка має важливе значення для захисту національних інтересів;
- "комп'ютерна злочинність" та "комп'ютерний тероризм".

Оскільки головним об'єктом інформаційного впливу залишається свідомість (а ще частіше підсвідомість), важливо попереджувати такі методи впливу на інформаційний простір України деструктивними силами. Також необхідно заохочувати створення якісного та перевіреного інформаційного контенту на базі українських ЗМІ, що враховували б історичний та культурний досвід українського народу.

Важливо підкреслити, що:

- Росія використовує інформацію як інструмент панування та ведення війни – цей висновок можна зробити як з аналізу офіційних документів Росії, так і з моніторингу її інформаційної практики;
- У ситуації, коли інформація стає дедалі більш озброєною, національні уряди та парламенти, а також міжнародна спільнота повинна шукати шляхи її роззброєння, коли вона використовується в зловмисних цілях;
- Оскільки безпека та роззброєння були ключовими принципами Гельсінського процесу в 1970-х роках, який став віхою для європейської безпеки, важливо дотримуватися підходу до роззброєння в інформаційному полі, тобто боротьби з агресивною практикою дезінформації в інформаційній сфері;
- Це «інформаційне роззброєння» повинно враховувати, що інструменти, що використовуються російською інформаційною війною, надзвичайно гнучкі.

З попередніх розділів очевидним став той факт, що важливими інструментами у розповсюдженні дезінформації та пропаганди стали засоби масової інформації. Також варто пам'ятати про важливість соціальних мереж, які часто виступають в ролі ЗМІ. З цього можна зробити висновок, що державі варто приділити увагу коректній та професійній роботі ЗМІ в Україні, що передбачає:

- Прозорість засобів масової інформації, зокрема Інтернет-засобів масової інформації, які можуть забезпечити відстеження шкідливих впливів та відповідальність інформаційних ресурсів;
- Прозорість політичних та інформаційних кампаній, особливо в період виборів; забезпечити, щоб інтернет-платформи робили технології, що забезпечують цю прозорість, доступними у всьому світі;
- Посилити законодавчі дії проти свідомого розповсюдження дезінформації та маніпуляцій з інформацією;
- Запровадити санкції (заборона на виїзд та замороження активів) проти учасників інформаційної війни;
- Запровадити санкції проти російських «медіа» компаній, які порушують попередні санкційні режими (тобто російських компаній, які захопили українські медіачастоти в Криму чи на Донбасі);
- Ввести спеціальні вимоги щодо брендування російських державних ЗМІ (вимагаючи від них розкрити інформацію про те, що вони «фінансуються урядом Росії»);
- Більш систематично приступити до медіаграмотності не лише у формальній, але й у неформальній освіті.

Основні проблеми організації протидії:

- Швидкість створення та розповсюдження руйнівного вмісту, яка не порівнянна зі швидкістю реакції. Суть проблеми полягає у суперечності між швидкостями та обсягами виробництва руйнівного вмісту та оперативною реакцією на нього. Приклад: статистика в Інтернеті, кількість відеозаписів про

злочини у порівнянні з запобіганням та покаранням? Зокрема, події «страсти заручників» та «покарання терористів».

- Злиття державного устрою та політичного режиму. За цих обставин інформаційні напади на державні установи маскуються політичною боротьбою, що ускладнює їх виявлення.
- Екстериторіальна загроза. Чинними особами та виробниками руйнівного контенту можуть бути громадяни будь-якої країни: як свідомі "агенти впливу", так і просто "корисні ідіоти".
- Політкоректність. Проблема політкоректності полягає у необхідності спотворення дійсності заради політичної доцільності. Іншими словами, це нездатність політичних лідерів сформулювати, яку саме загрозу несе в собі російська інформаційна пропаганда. Це спричинило допуск російських ЗМІ на інформаційний простір ЄС. Як результат, сьогодні всі учасники формату Нормандії для своїх виборців були або «маріонетками Вашингтона», або «мілітаристами, які рухають світ до війни, стимулюючи та заохочуючи агресію проти Росії з боку української хунти». За цих обставин Росія стала чинником внутрішньополітичного порядку на виборах у США та всіх європейських країнах [28].

Для того, щоб убезпечити населення від російського пропагандистського контенту в Україні вже створено існує Рада національної безпеки та оборони, що займається аналізом стану та готовності суб'єктів кібербезпеки до протидії кіберзагрозам.

Також для того, щоб зменшити поширення дезінформації так званими «корисними ідіотами», необхідно впроваджувати освітні проєкти, що б підвищували кібербезпекову грамотність як дорослих людей, так і дітей шкільного віку. Це дозволить культивувати вміння критично ставитись до інформації, що подається в ЗМІ та через соціальні мережі з юного віку.

Здається необхідним переглянути навчальні програми в університетах, особливо в галузі журналістики, міжнародних відносин та економіки. Сферу освіти слід розширити, включивши безпеку в Інтернеті, основи інформаційно-

психологічної війни, інформаційну політику та пропаганду. Адаптація академічних програм також повинна включати проблеми у сфері внутрішньої безпеки перед сучасними викликами та загрозами. В довгостроковій перспективі така політика обов'язково дасть свої плоди.

Основні цілі протидії інформаційним загрозам:

1. Зміцнення довіри до державних та міжнародних інституцій.
2. Підвищення обізнаності громадськості про цілі та вплив інформаційної агресії, структури та організації.
3. Формування критичного підходу до інформаційних та соціальних установок, що забезпечують психологічну стабільність громадян щодо наслідків руйнівного змісту.
4. Залучення великих мас людей до виробництва та просування „конструктивного” контенту.
5. Сформувати систему активного впливу на основних діювих осіб та обмеження їх можливостей, участь у просуванні деструктивного змісту.

Видається очевидним, що стратегія інформаційної війни української держави повинна включати оборонну та наступальну політику. Що стосується першої складової, то тут йдеться про дії, спрямовані на фізичний та психологічний захист населення, військ, уряду, інформаційної інфраструктури та супутників у космосі. Оборонна політика повинна включати: організацію діяльності структури формування оборонних систем та співпрацю з іншими державами з метою протидії інформаційній війні; оперативна протидія діяльності, впливам та проявам інформаційної політичної агресії, операціям інформаційно-психологічної війни; приведення засобів масової інформації та віртуальних спільнот до готовності ефективно протидіяти та реагувати на інформаційну агресію.

Дії держави у вищезазначених умовах можна розділити на три рівні: перший – геополітичний (це вплив на інформаційного агресора та обмеження інтенсивності та сили його нападу); другий – умова, що включає захист цілісності, ефективності та спроможності системи управління, інформаційної

інфраструктури, інформаційних ресурсів; третій – громадський (спрямована на захист стабільності та послідовності розвитку соціально-політичних відносин, свідомості громадян, цілісності кожної людини).

Ось чому найважливішими для української держави є: формування справді ефективної системи інформаційної війни, а також методу протидії інформаційним впливам з боку держави-агресора; розробка стратегії інформаційної війни за участю вчених, політологів та аналітиків, що спеціалізуються на інформаційній сфері; підтримка іміджу держави, покращення ефективного висвітлення правдивої інформації в засобах масової інформації та вдосконалення їх роботи загалом.

Основними методами протидії інформаційній агресії є:

- Співпраця та координація в інформаційній політиці – державна підтримка нових аналітичних чи медіаініціатив та проєктів, включаючи більш гнучкий підхід до надання грантів чи стипендії;
- Удосконалення навчальних програм в університетах в галузі журналістики, міжнародних відносин та економіки – включити в програму безпеку в Інтернеті, основи інформаційно-психологічної війни, інформаційну політику та пропаганду, проблеми у сфері внутрішньої безпеки перед сучасними викликами та загрозами;
- Обмеження та нейтралізація впливу пропагандистського повідомлення, а також послаблення потенційних союзників насамперед на власній території. Для цього потрібна співпраця неурядових організацій та державних структур, особливо дипломатії та правоохоронних органів;
- Комунікація між владними структурами та суспільством – неповнота інформації або двозначність у спілкуванні заповнюється різними видами спекуляцій та новинами з ворожих ЗМІ;
- Підвищення якості контенту в ЗМІ – правдивість, відкритість, прозорість, збалансованість подання інформації (представлення різних точок зору, а не нав'язування), факти віддалені від оцінок;

- Обмеження присутності російських ЗМІ в Україні. Ця функція дозволяє обмежити доступ деструктивного контенту до широкої цільової аудиторії та зменшити його вплив на соціальний та психологічний стан населення.

Найкращим способом протистояти інформаційній війні було б представити раціональні аргументи, підкріплені реальними доказами, щоб зруйнувати міфи та переконання, які запроваджуються деструктивними силами, щоб створити паніку та маніпулювати населенням. Підвищення обізнаності про Росію є життєво важливим компонентом збільшення частки оцінок, що базуються на фактах, та поінформованих думок у суспільстві, а отже, зменшує сприйнятливність різних маніпуляцій з боку Росії.

Приклад України показує, що Росія не відмовляється від своєї інформаційно-психологічної війни, яка є продовженням її агресивної зовнішньої політики. Ці дії є спробою компенсувати військову та економічну слабкість, але водночас еманацією багаторічної підготовки, досвіду та політичної волі для ескалації напруженості та захисту району, що розуміється як «близьке закордоння», а також для стримувати суперників, які вже перебувають на їх території.

Росія постійно робить спроби найняти за різними каналами журналістів, експертів, науковців, активістів, митців та спеціалістів для діяльності у різних секторах – вдома та за кордоном. Навколишнє середовище та особи, що відмежовуються від політики, особливо схильні до ризику. Основним мотивом тут може бути насамперед фінансовий фактор, а також ексклюзивна поїздка за кордон, стипендія чи отримання підтримки або нові можливості для кар'єрного зростання.

Спроби залякати журналістів та активістів, які розслідують зв'язки між організаціями, ЗМІ та політиками з Росією, є серйозним викликом для служб України та західних країн.

Необхідно обмежити та нейтралізувати вплив російського пропагандистського повідомлення, а також послабити потенційних союзників

Кремля насамперед на власній території. Для цього потрібна співпраця неурядових організацій та державних структур, особливо дипломатії та правоохоронних органів.

Основні помилки в інформаційній стратегії України:

- Особливу увагу привертає відсутність ефективної комунікації між владними структурами та суспільством. Українські аналітики часто наголошують, що крім насичених пафосом виступів провідних політиків, немає чіткого повідомлення про плани чи навіть умови прийняття рішень, особливо тих, які надзвичайно важливі для різних соціальних груп. Цей розрив у спілкуванні заповнюється різними видами спекуляцій та новинами з російських чи проросійських ЗМІ [19].

- Інша проблема – якість української журналістики. Одним з головних недоліків є все ще широко розповсюджена відсутність знань іноземних мов (що унеможлиблює безпосереднє використання іноземних джерел та спричиняє принципові недоліки в тлумаченні європейських подій) та невідповідність західним стандартам при підготовці матеріалів для преси (плагіат та порушення авторських прав), які стосуються якості повідомлення та, як наслідок, довіри до окремих ЗМІ [19].

Це, звичайно, похідне низького заробітку в галузі та відсутності фінансування для них. Це впливає на якість персоналу, а також на їх підхід до роботи. Це також означає, що, попри напружений конфлікт на Сході, багато журналістів все ще використовують російські ЗМІ для підготовки своєї інформації. Це особливо ясно, коли йдеться про висловлювання іноземних політиків про Україну чи Росію, які мають найбільший відгук в українському суспільстві.

Найвідомішим прикладом тут буде ставлення найбільших українських інформаційних агентств, які, складаючи звіт про виступ Ангели Меркель на мітингу Християнсько-демократичного союзу, повторили маніпульоване повідомлення російського агентства РІА «Новости», що «Європа хоче побудувати мир з Росією та співпрацювати з нею» [5]. Це було використано в

Україні для посилення негативних настроїв, особливо відчуття зради Заходу, тоді як слово «знову» відсутнє в заголовках.

Ще однією важливою умовою успішного просування інформаційної війни проти України є благодатне підґрунтя для проростання пропаганди на території України, це так звана «п'ята колона». Під цим терміном розуміють групу людей, що проводять відкриту або закриту підривну діяльність зсередини іншої групи або країни. в Україні існує російська «п'ята колона», яка складається з держпосадовців, журналістів, суддів, міліціонерів та, навіть, терористів або розвідників, що під прикриттям проживають в Україні, час від часу влаштовуючи провокації за вказівками Кремля [15].

Існування такої групи людей в Україні може погано позначитись на національній безпеці держави. Зі своєї сторони Україна намагається здійснювати певні кроки проти підривної діяльності всередині країни: це і люстрація держпосадовців, та закриття пропагандистських телевізійних каналів, що займалися розповсюдженням дезінформації та «промиванням мізків» звичайним громадянам. Так у 2014 році на початку тимчасової окупації Криму було вимкнено мовлення телеканалу «Інтер», що належить С.Льовочкіну. А в лютому 2021 року В. Зеленський підписав рішення РНБО, що стосується нардепа від «Опозиційної платформи – За життя» Тараса Козака та телевізійних каналів "112 Україна", NewsOne, ZIK. «Формально ці канали записані на того ж Козака. Де-факто їх вважають активами політика Віктора Медведчука – кума президента Росії Володимира Путіна та одного з очільників «ОПЗЖ» [41]. Згодом Генпрокурор І. Венедіктова підписала підозру в державній зраді Медведчуку та Козаку. Підозрюється, що Медведчук вступив у змову з РФ для видобутку нафти і газу в Чорному морі. А вже у 2021 травні року Медведчука відправили під домашній арешт на три місяці.

Хоч ця справа ще не закінчена і остаточних висновків можна чекати лише після повного закінчення слідства та судів, вже сьогодні зрозуміло, що це важливий крок в умовах інформаційної війни, що дозволить очистити інформаційне поле від небажаної пропаганди та дезінформації серед населення.

Хоч і сьогодні російські засоби масової інформації не представлені в Україні так широко як кілька років тому, все ще зберігається небезпека інформаційних атак. Вони можуть проводитися в соціальних мережах, через підкупних журналістів та ін. в цій ситуації неможливо взагалі позбутися намагань ворожої сторони щодо дезінформації та пропаганди, але можливо змінити ставлення населення до інформаційних фейків на більш критичне та підвищення якості вітчизняних ЗМІ та, відповідно, довіри населення до них.

Очевидно, що ці заходи повинні використовуватися на рівні з іншими кібербезпековими методами, що описані вище. Це дасть змогу досягти високих результатів та не лише протидіяти можливим загрозам, а й автоматично знижувати руйнівний вплив тих інформаційних потоків ворога, що все ж матимуть змогу поникнути в інформаційне поле України.

Україні потрібна система кібербезпеки, сумісна з партнерами НАТО-ЄС, адже захист в кіберпросторі є невід'ємною частиною національної безпеки.

Враховуючи значний прогрес та досвід НАТО у створенні та зміцненні механізму кібербезпеки держав-членів, Україна повинна стати активним учасником цих процесів безпеки. Таким чином, враховуючи євроатлантичні амбіції України, це допоможе зміцнити репутацію країни, а з іншого боку, встановити правові основи національної кібербезпеки. Так само це сприяє інтеграції до НАТО та розробці оптимальної моделі для безпечного захисту внутрішнього кіберпростору. В умовах гібридної війни та впровадження заходів електронного врядування аспекти кібербезпеки для України повинні бути предметом державної політики.

Тому Україна консолідує свої зусилля щодо імплементації стандартів НАТО, щоб бути повністю інтегрованою до глобальної системи кіберзахисту. Тим не менше, процес приєднання до системи колективної безпеки все ще йде повільно, що свідчить про те, що нинішні кібернетичні можливості не відповідають вимогам НАТО [26].

Проблема спільної протидії російській агресії України разом з західними країнами полягає також у закритості та непередбачуваності України. Вона не

відповідає західним стандартам та не відповідає їх ідеалам. Високий рівень корупції, неофеодалізм, недосконала правова та судова система. Важливим питанням також є олігархізація еліти, що стала домінуючою тенденцією та призвела до вибудовування корупційної держави. «Внаслідок цього відбулася зміна в системі нормативно-ціннісних орієнтирів політичної еліти – націо- та державотворчі установки, освіченість, інтелігентність, загальнонаціональні та громадянські інтереси поглинули егоїстичні, вузькогрупові інтереси корупційно-олігархічних груп. Це призвело до глибокої політичної кризи та, зокрема, кризи політичної еліти [34].» Наслідком цього є утворення феномену «псевдоеліти», що характеризується зовнішньою імітацією демократичних стандартів поведінки та внутрішньою відповідністю змісту та цінностям, що характерні для олігархічної, кланової, корупційної групи, яка ставить проблеми державотворення та політичної нації на другий план. О

Інтеграція в ЄС та НАТО можливе лише за умови подібності України з західними країнами та відсутність побоювань щодо можливих непередбачуваних проблем та виникнення «українського питання» на карті світу. В цьому велику роль також грає російський конфлікт, в умовах якого євро-атлантична інтеграція виглядає малоймовірною.

Проблема боротьби проти російської гібридної агресії потребуватиме подальшої спільної роботи США, Європи та України щодо побудови та підвищення ефективності системи стримування неоімперської політики Москви, в тому числі в гібридній сфері. Самостійна боротьба України проти інформаційних загроз РФ може не дати жодних результатів, адже російська інформаційна війна спрямована не лише на Україну, а й на інші країни світу, тому лише спільними зусиллями впливових акторів міжнародних відносин можна досягти нейтралізації негативного впливу ворожих інформаційних потоків.

Під час боротьби з інформаційними атаками Росії важливо не лише протидіяти їм на території України, а й звертатися по допомогу та співпрацю до інших країн-партнерів, адже очевидно, що інформаційні впливи Кремля

поширюються також на інші країни світу. Таким чином створюється погана репутація України та українців закордоном, що формує негативний імідж. Це також впливає на вірогідність вступу України до НАТО та ЄС найближчим часом. Іноземною пресою шириться інформація про негативні сторони України, її провали та недопрацювання, що нашттовхує на думку про відсталість та неспроможність українців будувати державу за західними цінностями. Такі інформаційні впливи також не висвітлюють жодних позитивних сторін та досягнень України, які безумовно існують, але світовій спільноті про них невідомо.

До кібератак слід ставитись дуже серйозно, а держава повинна інвестувати в наукові дослідження та розробку спеціалізованого програмного та апаратного забезпечення, здатного вести боротьбу в галузі кібербезпеки. Тим часом військові та цивільні фахівці повинні отримувати постійну освіту та навчання з кібербезпеки. Вебсайти, електронні листи та внутрішні мережі стратегічних установ повинні бути добре захищені шляхом встановлення найкращого антивірусного програмного забезпечення. Працівники повинні бути навчені розпізнавати та уникати можливих загроз. Існування команд для участі в контрреволюційній боротьбі з повстанцями може зробити вирішальний внесок у боротьбу з гібридними загрозами. І останнє, але не менш важливе: існування антипропагандистського агентства для підвищення обізнаності про фальшиві новини є обов'язковим для протидії гібридній війні.

Розвиваючи свою систему кібербезпеки, Україна орієнтувалась на модель ЄС у сферах захисту мереж та протидії кіберзлочинності та у своїй кіберзахисті на підході НАТО, що можна побачити у визнанні кіберпростору як однієї із сфер інтересів держави.

Хоча Україна помітно досягла певного прогресу у зміцненні своїх кіберможливостей, оборона не на рівні, який очікується від країни, яка перебуває під обстрілом російської кібервійни. Є проблеми у спілкуванні та координації між урядовими установами, бракує фінансового стимулу для

залучення найкращих фахівців до роботи в уряді, і існує значна проблема співпраці державного та приватного секторів, що є вирішальною для успіху.

Тим не менше, Україна намагається вчитися на своїх помилках, і що важливо для західних партнерів – вона пропонує нові знання. Ось чому американські та європейські органи кібербезпеки регулярно просять проаналізувати основні загрози в Україні, щоб шукати досвід, який можна застосувати «вдома». У 2019 році, через три роки після того, як Росія зірвала вибори президента США у 2016 році, європейські чиновники були стурбовані тим, що вибори до Європарламенту будуть наступними. Отже, в ЄС уважно спостерігали за виборами президента України, розуміючи тенденції.

Очевидно, що посилення українського кіберзахисту неможливе без фінансової та навчальної допомоги західних партнерів. У цій співпраці Служба безпеки України та Державна служба спеціального зв'язку та захисту інформації України були основними отримувачами допомоги від Цільового фонду. На весь проект НАТО виділило понад 1 мільйон доларів. Партнери з НАТО (з Румунією як провідною державою, що діє через Російську розвідувальну службу) надали додаткові фінансові внески та внесли досвід, що призвело до спільних навчань та тренінгів з кіберзахисту, зосереджуючись на тому, як реагувати на великі кібератаки [37].

Надалі важливо удосконалювати систему якості освіти у кібербезпекових напрямках, для цього необхідно дослідити досвід інших держав та відштовхуючись від цього досвіду будувати свою систему освіти.

Варто дослідити можливі сценарії розвитку інформаційних технологій та як вони впливатимуть на питання міжнародної кібербезпеки. Цю ініціативу варто розпочати за партнерства інших країн, що допоможе ефективно дослідити проблематику та знайти можливий вихід на міжнародному рівні.

ВИСНОВКИ

Інформаційна безпека являється пріоритетною функцією держави, адже це ключовий елемент національної безпеки. Вона передбачає забезпечення якісного та всебічного інформування громадян, а також надання вільного доступу до різноманітних джерел інформації. Ключовими компонентами інформаційної безпеки також є: контроль за непоширенням дезінформації, сприяння цілісності суспільства, збереження інформаційного суверенітету, протидія негативним інформаційно психологічним пропагандистським впливам та захист національного інформаційного простору від маніпуляцій, інформаційних війн та операцій.

Досліджено природу та трансформацію інформаційних війн. Перші прояви ведення інформаційного протиборства були зафіксовані ще за давніх часів, коли міфи і легенди використовувалися для того, щоб звеличувати, нажахати або навіювати різного роду інформаційні посили. З розвитком інформаційних технологій та глобалізацією суспільства, інформаційна складова протиборства стала чи не найважливішою на шляху до досягнення цілей.

В умовах швидкого розвитку інформаційних технологій та все більшого використання сучасних гаджетів населенням різного віку, статі та соціального положення критично важливим стало запобігання поширення ворожого, неправдивого та пропагандистського контенту на території кожної окремої держави. Це питання набуває загальнодержавного значення на рівні з національною безпекою.

Проаналізувавши особливості інформаційної війни Росії проти України, виявлено основні методи, що використовувалися ворожими силами: захоплення медіапростору, «перетасовка» фактів, дезінформація, наклепи на українську владу та її політику, виправдання дій Росії благими намірами. Виявлено, що пропаганда в українських ЗМІ допомогла Росії виправдовувати свої дії та вводити в оману населення України, Росії та інших країн світу у найгострішу фазу конфлікту, що негативно вплинуло на позиції України у цій війні.

З'ясовано причини, чому дії країни-агресора, Росії, були результативними та як їм можна протидіяти в подальшому. Найважливішими заходами протидії є: ефективна комунікація між владними структурами та суспільством, підвищення якості журналістики та довіри людей до неї, розробка та впровадження новітніх конкурентоспроможних засобів кіберзахисту, удосконалення системи освіти та підвищення її якості у галузі кібербезпеки. Вартим уваги є питання співпраці України з іншими країнами на умовах взаємовигідного партнерства, адже Україна може запропонувати поле для навчання спеціалістів у цій галузі на практиці, в той час як взамін ми отримаємо технології, знання, навички, спеціалістів.

На підставі інформації поданої в перших двох розділах роботи, у третьому розділі зроблено висновки щодо причин, чому дії країни-агресора мали результати та як їм можна протидіяти в подальшому. Доведено, що найважливішими заходами протидії є: ефективна комунікація між владними структурами та суспільством, підвищення якості журналістики та довіри людей до неї, розробка та впровадження новітніх конкурентоспроможних засобів кіберзахисту.

Виходячи з викладеного матеріалу, інформаційна безпека держави характеризується ступенем її захищеності. Ключову роль грає стійкість головних сфер життєдіяльності по відношенню до небезпечних інформаційних впливів. Інформаційна безпека визначається здатністю нейтралізувати шкідливі інформаційні впливи. Національна безпека повинна гарантувати захищеність життєво важливих інтересів громадян, суспільства та держави в інформаційній сфері.

СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ:

1. Еляшевська, Н. (2015). Вразливість України до інформаційної війни
2. Інформаційна війна з Україною Росії коштує мільярди [Електронний ресурс] // Антена онлайн. – 2017. – URL: <https://antenna.com.ua/archives/11172>.
3. Кіхтан В.В., Качмазова З.М. Інформаційна Війна: Поняття, Зміст І Основні Форми Прояви
4. КРИМ 94. Частина 3 «Як ділився Чорноморський флот «по-братерськи» [Електронний ресурс] // НЕЗАЛЕЖНИЙ АНАЛІТИЧНИЙ ЦЕНТР ГЕОПОЛІТИЧНИХ ДОСЛІДЖЕНЬ Борисфен Інтел. – 2013. – URL: <http://bintel.com.ua/uk/article/kak-delilsja+-chernomorskij-flot-po-bratski/>.
5. Лубкович, І. М. (2014). Місце українських медіа в інформаційній війні 2013-2014 рр. Наукові записки інституту журналістики, № 56
6. Малик І. Р. Інформаційні війни в Україні: історія, сучасний стан та перспективи.
7. Манойло А.В. Інформаційно-психологічна війна: фактори, що визначають формат сучасного збройного конфлікту. К - (2005). - Матеріали V Міжнародної науково-практичної конференції «Інформаційні технології та безпека», вип. №8, 2005 р с. 73-80
8. Маруненко О. Зовнішні і внутрішні інформаційні війни у медійному просторі України / Олександр Маруненко // Освіта регіону. Політологія, психологія, комунікації. Український науковий журнал
9. Називай агресію «захистом»: принципи інформаційної війни проти України [Електронний ресурс] // Радіо Свобода. – 2014. – URL: <https://www.radiosvoboda.org/a/25293307.html>.
10. Освіта як об'єкт інформаційної війни Росії проти України і як ресурс протидії такій війні [Електронний ресурс] // Інформаційний центр “Майдан Моніторинг”. – 2015. – URL: maidanua.org/2015/03.
11. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи...

12. Рішення Ради Національної Безпеки і Оборони України Про стратегію кібербезпеки України <http://www.president.gov.ua/documents/472017-21374>.
13. Сенченко М. Запорука національної безпеки в умовах інформаційної війни / м. Сенченко., 2014. – (Вісник Книжкової палати). – (6).
14. Сьомін С. В. Україна в третій світовій війні / с. в. Сьомін., 2000. – (Київ). – (4).
15. Укрінформ – В Україна дослідять, хто з експертів та ЗМІ працює на Путіна. URL: <http://www.ukrinform.ua/block-lastnews/page-4>
16. Як виграти інформаційну війну [Електронний ресурс] // Українська правда. – 2006. – URL: <https://www.pravda.com.ua/articles/2006/05/29/3111800/>
17. Васильев А. Д., Подсохин Ф. Е. [Информационная война: лингвистический аспект](#) // Политическая лингвистика. — 2016. — № 2 (56). — С. 10—16.].
18. Кравчук рассказал, как Россия в 1992 году собиралась атаковать Одессу военными кораблями [Електронний ресурс] // Хвиля. – 2015. – URL: <https://hvylya.net/news/digest/kravchuk-rasskazal-kak-rossiya-v-1992-godu-sobiralas-atakovat-odessu-voennymi-korablyami.html>.
19. Маклюэн М. Понимание Медиа: Внешние расширения человека/ Пер. с англ. В. Николаева; Закл. ст. М. Вавилова. – М.; Жуковский: «КАНОН-пресс-Ц», «Кучково поле», 2003. – 464 с.
20. [Об информационной войне и Русском фронте Первой мировой.](#) [Електронний ресурс] // Битва гвардий. – 2021. – URL: <http://btgv.ru/history/great-war/%D0%B1%D0%B8%D1%82%D0%B2%D0%B0-%D0%BD%D0%B0-%D0%B2%D1%81%D0%B5%D1%85-%D1%84%D1%80%D0%BE%D0%BD%D1%82%D0%B0%D1%85/about-the-information-war-and-the-russian-front-of-the-first-world-war/>
21. Почепцов Г. Г. [Информационно-психологическая война](#) – 2000 - СИНТЕГ

22. Расторгуев, С. П. (1997). Информационная война как целенаправленное информационное воздействие информационных систем. Информационное общество
23. Расторгуев С. П. Очень краткая лекция по теории информационной войны [Электронный ресурс] / С. П. Расторгуев. – URL: <http://www.infwar.ru/article.php?num=1>
24. Руцькой О. В., Независимая газета, 7 квітня 1992, стор. 1
25. Тимур Андриевский – Гибридная война: сущность и базовые стратегии.
26. Clifford Reid, “Reflexive Control In Soviet Military Planning,” Soviet Strategic Deception, Ed. Brian Dailey And Patrick Parker, Lexington Books, 1987, P.294
27. Dubov D. Cyber space as a new dimension geopolitical rivalry. Monograph. 2014. 328 pp.
28. Fleming Brian P. (2011-05-19). ["Hybrid threat concept: contemporary war, military planning and the advent of unrestricted operational art". United States Army Command and General Staff College.](#)
29. How to resist information aggression: the experience of Ukraine [Электронный ресурс] // INTERNATIONAL CENTER FOR COUNTERING RUSSIAN PROPAGANDA. – 2020. – URL: <https://www.iccrp.org/en/how-to-resist-information-aggression-the-experience-of-ukraine/>.
30. Kennan Cable No.7: A Closer look at Russia’s “Hybrid War” [Электронный ресурс] // Kennan Institute. – 2015. – URL: <http://www.wilsoncenter.org/sites/default/files/7-KENNAN%20CABLEROJANSKY%20KOFMAN.pdf>.
31. М. McLuhan. Culture is Our Business. — New York, 1970 (цит. по [переизданию 2015 года](#), с. 66
32. Martin C. Libicki - Cyberdeterrence and Cyberwar (2009
33. Putin's information warfare in ukraine: soviet origins of russia's hybrid warfare [Электронный ресурс] // RUSSIA REPORT. – 2015. – URL:

<http://www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare>.

34. Postolovska O.O. The Political and Cultural Characteristics of the Transformation of Modern Ukraine's Political Elite.

35. Rosyjska wojna informacyjna na Ukrainie [Електронний ресурс] // Defence 24. – 2016. – URL: <https://www.defence24.pl/rosyjska-wojna-informacyjna-na-ukrainie>.

36. RUSSIA'S HYBRID WAR IN UKRAINE (2014-2018) – CĂTĂLIN ALIN COSTEA

37. Strowell, Joshua. "[What is Hybrid Warfare?](#)". Global Security Review. Retrieved 26 July 2018.

38. Tetyana Demyanchuk - Whither cybersecurity of Ukraine? A short assessment

39. The Crimean War 1854/56 and Australian Involvement [Електронний ресурс] // Digger History. – 2011. – URL: <http://www.diggerhistory.info/pages-conflicts-periods/other/crimea.htm>.

40. The information war is here [Електронний ресурс] // New Eastern Europe. – 2020. – URL: <https://neweasterneurope.eu/2020/12/12/the-information-war-is-here>.

41. YouTube blocks access to Ukrainian TV channels tied to Kremlin ally, Ukraine govt says – Reuters – URL: <https://www.reuters.com/world/europe/youtube-blocks-access-ukrainian-tv-channels-tied-kremlin-ally-ukraine-govt-says-2021-04-24/>