МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
Факультет міжнародних відносин
Кафедра журналістики

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
Васильченко В’ячеслав Миколайович
_____
«___» _____ 2022 р.

ДИПЛОМНА РОБОТА

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»

ДЕЗІНФОРМАЦІЯ ЯК ІНСТРУМЕНТ ГІБРИДНОЇ ВІЙНИ В УКРАЇНІ

Виконавець: Тверда Олександра Віталіївна _____
Керівник: канд. філол. наук, доц.
Васильченко В’ячеслав Миколайович _____
Нормоконтролер: канд. пед. наук, доц
Остапчук Світлана Сергіївна _____

Київ – 2022

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Процеси, що супроводжуються конкурентною боротьбою держав у геополітичному просторі, сприяють виникненню нових викликів та загроз безпеці національних інтересів усіх держав. Однією з таких загроз є «гібридні війни», тому вивчення явища «гібридних війн», характеристики їх найважливіших аспектів є предметом наукового інтересу і знаходиться в центрі сучасних досліджень.

Слід наголосити, що «гібридні війни» - досить складне явище, оскільки за своєю природою мають на увазі використання військових та невійськових технологій одночасно чи по черзі, залежно від об'єкта впливу. До військових технологій належать використання сил спеціальних розділів, військових компаній, що мають приватний статус, угрупувань терористичного походження тощо. До невоєнних технологій чи інструментів належать розвідувально - підривна діяльність спецслужб, «інформаційні війни», «кібервійни», «санкційні війни», медіа-ресурси, Інтернет - простір, соціальні мережі тощо.

У процесі «гібридної війни» можуть вестись і звичайні бойові дії, партизанська тактика, терористичні акти, кримінальне насильство та примус. Вся ця різноманітна діяльність може здійснюватись різними методами, або навіть одним підрозділом, але з однією метою – для отримання найбільшого, синергетичного (позитивного) та психологічного ефекту». На сучасному етапі, в рамках своїх геополітичних та геоекономічних інтересів, «гібридні війни» ведуть між собою світові та регіональні держави, причому на чужій території, тобто в окремо взятому регіоні або в конкретній країні, чужими руками, при цьому заперечуючи свою причетність у всьому.

Слід зазначити, що гібридні конфлікти загалом координують умисні дії, користуючись складнішою стратегією, чия інтенсивність змінюється на різних стадіях конфлікту і який прагне дестабілізувати процеси в державі. Мета -

знищити державу, дестабілізуючи економіку, розлад і незадоволення населення, порушуючи права національних меншин, створюючи умови, що бадьорять керовану і безконтрольну міграцію, цивільне придушення опору і деструкцію критичної інфраструктури. Це обумовлено використанням розвідслужб, дій спеціальних одиниць. Що продемонстровано в сьогоднішній боротьбі в України, у минулому в Грузії та ін. Методи, використані в гібридних конфліктах, - часто вдосконалені, обумовлені впровадженням нових технологій, які дозволяють більше проникнути в критичні елементи.

Слід зазначити, що алгоритми гібридної війни — це більше, ніж атаки на життєво важливі системи, такі як комунікації, інфраструктура чи транспорт. Державні та недержавні організації все частіше знаходять прогалини в ідеологіях та інститутах або використовують соціальне невдоволення для початку нових воєн. Отже, «гібридна війна» — це високотехнологічний конфлікт. Це просування політики держави чи коаліції, політичних груп, транснаціональних корпорацій та неурядових організацій. Метою конфлікту є нав’язування опонентам точки зору через інтегрований адаптаційний та асиметричний синхронний деструктивний вплив на опонентів у багатовимірному просторі та в різних сферах життя.

Гібридна війна раціонально поєднує звичайні та нетрадиційні компоненти, наголошуючи на кількох джерелах і режимах атак, сукупному впливі результатів і високому рівні невизначеності щодо того, якими можуть бути кінцеві стратегічні цілі для ворогів. Основними цілями гібридних конфліктів є контроль над людьми, вплив на суспільні настрої та маніпулювання, які приймають рішення в державі. Ворог хоче маніпулювати цінностями, мотиваційними факторами, культурними основами та стратегічно важливою інфраструктурою країни. Це може бути завдяки комплексному застосуванню ефектів з використанням м’якої і жорсткої сили. Тому об’єктами є важливі складові держави – соціальна, дипломатична, технологічна, енергетична, фінансова, кібернетична, політична соціальна, інформаційна та

інші сфери. Порушення яких призводить до бажаного результату, а саме: важких деструктивних системних змін у структурі функціонування держави.

Отже, у контексті вищесказаного дослідження питання «гібридних війн» набуває актуальності, особливо в наш час.

Багатьма вченими було досліджено питання та його аспекти: П.Мансур, Френк Г. Хоффман, Майкл Айшервуд, Шейн Рівс, Роберт Барнсбі.

Мета дослідження - дослідити та проаналізувати питання «гібридних війн» та їх вплив на національну безпеку України.

Поставлена мета передбачає вирішення наступних **завдань:**

1. Дослідити теоретико-методологічні основи вивчення проблеми «гібридних війн» та дезінформації на сучасному етапі
2. Проаналізувати «гібридні війни» та їх вплив на національну безпеку України
3. Розглянути питання дезінформації як загрози національній безпеці України
4. Запропонувати інструмент протидії дезінформації в Україні

Об'єктом дослідження є гібридна війна та інформаційна безпека на території України.

Предметом дослідження є протидія поширенню дезінформації та пропаганди в інформаційному просторі.

Методи дослідження: На різних етапах роботи, відповідно до поставлених завдань були використані спеціальні та загальнонаукові методи, а саме метод аналізу використано при опрацюванні нормативно-правової бази України, що стосується поширенню дезінформації та боротьби з нею, історичний метод дав змогу простежити основні етапи розповсюдження дезінформації та формування інституційних механізмів для ефективної протидії цій загрозі на теренах України; метод узагальнення використано для виявлення головних загроз та викликів в умовах розквіту сучасних технологій.

Наукова новизна отриманих результатів. Полягає у проведенні загального аналізу виникнення гібридних конфліктів в Україні. Дослідження терміну «гібридна» війна, конфлікт. Розглядаються сучасні інформаційні

технології як засіб впливу на масову свідомість та визначаються подальші дії щодо протидії впливу інформаційних технологій на масову свідомість.

Практичне значення одержаних результатів полягає в привернені уваги до проблеми гібридних конфліктів, розроблення способів та заходів припинення гібридних конфліктів, а також результати дослідження можна використовувати в діяльності з планування та проведення спеціальних заходів для просування в освітніх установах.

Структура роботи. Дипломна робота складається зі вступу, 3 розділів, висновків до розділів, загальних висновків, списку використаних джерел, додатків. Загальний обсяг роботи становить 89 сторінок, основний текст викладено на 81 сторінці.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ВИВЧЕННЯ ПРОБЛЕМИ «ГІБРИДНИХ ВІЙН» ТА ДЕЗІНФОРМАЦІЇ НА СУЧАСНОМУ ЕТАПІ

1.1. Теоретичні аспекти вивчення проблем «гібридних воєн» та дезінформації

Свідомість пересічної особистості сьогодні перебуває під шаленою напругою із-за штучно навіяних суперечностей. Тотальний наступ на пересічну особистість у вкрай агресивній формі сьогодні отримав загальну назву – гібридна війна. У залежності від класифікації її параметрів ми маємо справу: з інформаційною війною, якщо для цього використовується інформаційний простір, наприклад, ЗМІ; кібервійною – якщо у цьому задіяні засоби Інтернету та інші мережі, наприклад, типу «Фейсбук» або «Твіттер»; медіавійною – якщо в якості головних інструментів впливу на людину використовуються специфічні медіазасоби. Гібридною війна стає завдяки нечітким методам впливу на людину. Загальний характер такого впливу – маніпуляційний [1, с. 56].

На рівні підсвідомості людини він збуджує сегменти архетипів страху і невпевненості у собі й у безпеці, вразливості умов власного життєустрою у просторі територіальної громади і країни в цілому. Наприклад, стверджується, що Україна – це не самостійне утворення і що вона в принципі не може бути суверенною і незалежною державою. На рівні свідомості людини вплив забезпечується тиском соціальної або так званої фенотипічної інформації. При цьому особливістю проявлення сили медіа-джерел над особистістю є те, що пряме командування її поведінки змінюється на психологічне навіювання і, як наслідок, проявляється на практиці безумовною покорою особистості телеглядача або навіть певної маси населення пропагандистським закликам. Останні зазвичай спрямовані на утворення у розумінні особистості зміненого

суспільного абсолюту, наприклад, способу життя людини або негативного ставлення до влади, як такої.

На рівні надсвідомості людини ми спостерігаємо наслідки реакції пересічної особистості на впливи гібридної війни завдяки замінам домінанти. Надсвідомість завжди орієнтована на задоволення домінуючої потреби, конкретний зміст якої каналізує напрям «психічного мутагенезу».

Таким чином, «психічні мутації» спочатку носять непередбачуваний, але невипадковий характер. В цьому сенсі звернемо увагу на основні властивості домінантного вогнища, що встановлені О. Ухтомським: підвищена збудливість, інерція в часі (домінанта існує, хоча роздратування завелике) і, найголовніше, здатність інтегрувати зовнішні подразники, «самопідживлюватися ними» [1, с. 44].

Атрибутивна властивість домінанти полягає в утриманні людини у стані безперервного збудження. Домінантний осередок здатний інтегрувати зовнішні подразники до цієї домінантної потреби дію усіх інших подразників. При цьому виявляється, що «немає сенсу входити в сварки та дебати тому, що, якщо склалася домінанта, її не подолати словами і переконаннями, – вона буде ними тільки підкріплюватися. Адже, що домінанта завжди самовиправдовується, і логіка – слуга її», – писав О. Ухтомський [1, с. 65]. Це означає, що надсвідомість завжди «працює» на задоволення потреби, що стійко домінує в ієрархії мотивів даного суб'єкта. Гібридна війна спеціально вводить у надсвідомість пересічної людини хибний орієнтир і робить його домінуючою потребою. Ефект значно зростає, якщо агресору вдалося вплинути на масу людей, як це було у випадку з окупацією Криму.

Так, наприклад, за спостереженням В. Нікитенко, у центрі уваги американської нації є домінування у світі, європейської – гуманізм, арабо-ісламської – релігія, китайської – продовження роду, православно-слов'янської – продукування духовності, індійсько-індуїстської – збереження кастової ієрархії, японської – робота, латиноамериканської – пошук ідентичності і утвердження власної індивідуальності, африканської – забезпечення

продовольчої проблеми [2, с. 24]. Ясно, що кожна з них націлена на захист власної потреби, у першу чергу, а вже потім звертається до планетарних потреб. Цим моментом можна пояснити важкий процес прийняття на національному рівні міжнародних угод, що стосуються екологічних проблем.

Залежно від того, які властивості притаманні даному соціуму, заангажованою гібридними технологіями людиною здійснюється вибір власної поведінки у новостворених умовах. Процеси адаптації – це врешті архетипи соціальної поведінки, за допомогою яких людина несвідомо конструює свою життєву реальність, свій життєвий шлях, зберігає той спільний для людини і соціуму простір сенсу, втрата якого ініціює життєву кризу індивіда й актуальну потребу в будь-якому возз'єднанні з соціумом.

Жодний індивід, жодна соціальна група неспроможні вільно, лише за власним бажанням, винайти нові (такі, яких би не було в архетипі) форми вирішення конфліктів і дисонансів.

Для того, щоб збагнути реальні загрози в інформаційному простору України треба надати попереднє визначення відповідних основних понять, які супроводжують поняття «інформаційна війна» та «гібридна війна», що на сьогодні вже можуть вважатися загальнозрозумілими в своїх основних характеристиках [2, с. 21].

Терміни «гібридна війна» разом з такими термінами, як «інформаційна війна», «ядерна війна», «холодна війна», «кібер – війна» застосовується все частіше в результаті розробки інформаційних та комунікаційних технологій, концепція цього терміна розширюється. На жаль, слід зазначити, що в останні роки термін гібридна війна все частіше використовується у зв'язку з нашою країною. Незважаючи на широке використання наукового терміна «Гібридна війна», досі немає чіткого визначення терміна. Найчастіше використовується синтетичне, інтеграційне визначення, яке включає активні військові дії, використовуючи спеціальну зброю (орієнтовану на фізичне утилізацію противника та його людську силу) та наборі певних кроків агресора до жертви, щоб дискредитувати його в світовій спільноті, власний народ, розділяють

політичну еліту та суспільство в цілому. Такі дії можуть вразити набагато сильніший удар, ніж військова вторгнення, оскільки їх мета полягає у формуванні певних стереотипів та ставлення та масової свідомості шляхом маніпулятивного впливу. Важливим прикладом ілюстрації цієї тези є сучасна ситуація в Україні [2, с. 5].

Зауважимо, що сучасні політичні та нейролінгвістичні технології забезпечують широкий спектр методів та методик маніпулятивного впливу на свідомість. Ці тенденції визначають важливість вивчення явища гібридної війни та методів її керівництва з метою створення ефективного механізму боротьби з такою війною. Аналіз останніх досліджень та публікацій. Аналіз сутності гібридної та інформаційної війни розглядався як іноземними, так і вітчизняними вченими у своїх наукових працях.

Серед відомих вчених, які вивчають явище інформації та гібридної війни належать: А. Манойло, П. Бергер, З. Бзежинський, Абдєєв Н. Вінер, Г. Лассуел, М. Постер, , С. Хантінгтон та ін., Е. Андрєєв, О. Деркач, Д. Фролов, Е. Тоффлер, Ф. Хоффман, Д. Ласік, Дж. Девіс, Ф. Ван Каппен, В. Бебик, Я. Жарков, О. Литвиненко, В. Петрик, М. Присяжнюк, І. Рабінович, Д. Фельдман, Ю. Шайгородський, Г. Почепцова. В даний час, однак, немає чіткого переліку методик та методів гібридної війни в літературі, що робить дослідження умовним щодо актуальності цього дослідження.

Важливо розглянути питання комплексно, аналізуючи зміст поняття «гібридна війна» та методів її ведення, з урахуванням сучасного етапу суспільного розвитку – в умовах інформаційного суспільства.

На думку теоретиків гібридної війни, сучасні конфлікти відбуваються у чотирьох споріднених сферах: фізичні, інформаційні, когнітивні та соціальні. Інформаційна сфера інтегрована, що конфліктні партії намагаються впливати на користь своєї перемоги. Поняття «гібридна війна» було введено американським вченим М. Маклюеном, який вважав засоби комунікації новим ресурсом держави та довів, що сучасні війни відбуваються в інформаційному просторі [3, с. 81].

1. Наразі існують різні можливості визначити суть гібридної війни:
2. Військова стратегія, яка поєднує в собі звичайну війну, невелику війну та кібер - війну;
3. Атака використання ядерної, біологічної, хімічної зброї, імпровізованої зброї на терористичних атаках та інформаційному тиску;
4. Складна та гнучка динаміка бойового простору, яка дозволяє швидко реакцію та адаптувати учасників протистояння;
5. Сучасний тип партизанської війни поєднує в собі сучасні технології та методи мобілізації (Білл Немет, підполковник військово - морської піхоти США);
6. Основний метод асиметричної війни, який проводиться на трьох умовних фронтах - серед населення зони конфліктів, населення в Тулі та міжнародній спільноті (полковник американської армії Джек Маккуен) [4, с. 22-39].

Ф. Гофман представляє таке визначення гібридної війни – як повного арсеналу всіх видів війни, включаючи звичайні можливості, нерегулярні тактики та утворення, терористичні дії, пов’язані з насильством та кримінальними заворушеннями [5, с. 4]. Вчений зазначив 5 структур гібридної війни: модальність напроти структури, , синтез, складність,одночасність та злочинність [6, с. 138].

На нашу думку, компоненти гібридної війни включають використання методів класичної війни (збройних військових операцій), інформації або інформаційно-психологічної, партизанської війни, «Кібер - війна», елементи тероризму та підрив, економічний та дипломатичний вплив.

Гібридна війна небезпечна, оскільки межі війни, сценарії її початку та кінця фактично видаляються, часто важко визначити ворога, змінювати стан військових на мирний конфлікт часто не вирішиться, в майбутньому ситуація може погіршитися [5, с. 6]. В даний час поняття «гібридної війни» та «загрози гібридної війни» вже були введені в офіційну термінологію західної військової політики. Тому в заключному документі, прийнятому в необхідність

підготувати звіти про військовий альянс Північної Атлантики, щоб «переконатися, що НАТО зможе зіткнутися з конкретними проблемами, які представляють загрози гібридної війни, пов'язаної з відкритими та закритими військовими, воєнізованими та цивільними заходами» [7, с. 25].

Члени Альянсу вважають гібридну війну широким набором дій противника, таємними операціями, що проводяться партизанськими групами з участю цивільних компонентів, а також боротьбою з пропагандистськими кампаніями, кібератами та місцевим сепаратизмом. У Латвії був створений навіть спеціальний навчальний центр (стратегічний центр передового досвіду), який виконує вправи в галузі спілкування та гібридної війни.

Переважна більшість авторів погоджуються з тим, що головним компонентом Гібридної війни є інформаційна війна. Це також свідчить про практику. Таким чином, постійний розвиток масажної системи призводить до протирання кордонів, широких можливостей маніпулятивного впливу на свідомість населення конкурентної країни шляхом накладення власних ідей. У українсько-російській інформаційній війні це є боротьбою так званої. Російський світ (ідеологія відновлення радянської системи) та Постмайданська Україна (з новими політичними проектами та постколоніальним синдромом) [8, с. 50].

Слід зазначити, що термін «інформаційна війна», що використовується як один з перших Т. Рон в аналітичному звіті для Boeing «Системи зброї та інформаційної війни» у 1976 р. [9, с. 115]. З цього моменту знання полягає в тому, що інформація може бути зброєю. І через те, що розвиток європейських та США економіки базується на новаторській інформаційній та телекомунікаційній технології, цей сектор стає особливо вразливим на момент війни навіть у період миру. Існує два основні напрямки впливу інформаційної зброї: вплив на інформаційні та ворожі системи та вплив на свідомість людей. Перший напрямок також називається Кібер - війною під час нападу на технічне обладнання та їх програмні систем. Наступне направлення - застарілі методи

пропаганди, контр пропаганди та протиріччя, які досягли безпрецедентних вимірів з точки зору витонченості та впливу маси на людський розум.

Знаменитим поняттям є: «... це такий конфлікт, завданням якого виступає захист своєї інформації та систем інформації, маніпулювання знаннями противника або її хиблення, зменшення можливостей протиборчої сторони в доступі і обробці інформації» [10, с. 3].

В даний час зрозуміло, що якщо Інтернет до недавнього часу, він все частіше набуває ваги на агітацію, пропаганду, яка характеризується значною агресивністю. Традиційні засоби масової інформації все частіше працюють з джерелами Інтернету як джерела інформації та засобів впливу на мислення громадян. Інформація в Інтернеті стає все більш популярною, швидко поширюється і має соціальне значення.

Мета інформаційної війни - керувати процесом зміни свідомості людей, їх світогляду, ставлення до суспільства та держави; Небезпека для людей - це втрата власної волі та державі - її суверенітет. Це завжди було метою кожного завойовника, але тепер його можна досягти іншим способом (навіть цей термін також з'явився: «м'яка сила» - м'яка сила, введена американським політологом Дж. Найком).

Однак ці засоби можуть в деяких випадках бути більш небезпечним, оскільки жертва м'якого тиску може не усвідомлювати шахрайства, це може бачити результат лише тоді, коли, буде пізно. У той же час ця зброя має величезний характер забою. Безкоштовно та важко контролювати розповсюдження інформації в Інтернеті спричиняє багато проблем спеціальних послуг з усіх держав з очевидних причин. Лавина інформації (і дезінформації) може завдати шкоди кожній державі (аж до революційного вибуху та повалення уряду) [10, с. 7].

Цікава думка А. Дорошенка про те, що інформаційна війна з'являється на поточному етапі у формі мережево-центральної війни, завданням якої є вбивство ідентичності, тобто руйнування національної держави-центральної ідентичності опонентного стану такого Держава, коли про нього можна сказати

лише про це нелюдський. і ворожий. Ідентичність полягає у переконанні більшості жителів власної країни або навіть частини мешканців противника щодо поганих намірів противника щодо власних жителів. Тема такої війни - це маса та індивідуальна свідомість. Слід зазначити, що вплив на інформацію може бути здійснено на основі фону інформаційного шуму, а також в умовах вакууму інформації. [11, с. 169].

Основні інструменти гібридної війни включають такі інформаційні заходи: засоби військової та політичної дезорієнтації противника; дезінформація про власні ресурси; Дії, спрямовані на запобігання, закриття каналів, що передають дані задля дезорієнтації та дезорганізації, збільшення аури напруги в суспільстві України від частих очікувань нападу й великого наступу по лінії фронту й дії на свідомість багатьох українців деморалізувати та навіяти панічні настрої [12, с. 306].

Постійне збільшення інформаційних потоків унеможливлює їх контроль будь - якого стану. Тобто головним завданням в момент протидії в сфері інформації виступає контроль потоку інформації, як правильно зазначає О. Дугін [13, с. 501], але перевірте алгоритм потоку інформації, що дозволяє її розшифрувати, і, таким чином, захист суспільства та його інститути управління.

У рамках аналізу сутності гібридної війни використовується термін «психологічна війна», вперше використовується британським істориком Дж. Фуллером на початку 20 століття. В даний час під час навчання військового персоналу в США офіцери вивчають тактику та стратегію психологічних операцій, які найчастіше використовуються під час мирних операцій [15, с. 89].

Інститут національних стратегічних досліджень США та деяких західних експертів, аналізуючи окремі елементи інформаційної війни, розрізняють керівництво психологічної війни, завданням якої є маніпуляція мас до: принести шкідливі думки та думки в громадськість і індивідуальна свідомість ворога; дезорієнтація та дезінформація мас; ослаблення певних переконань,

основи; залякування людей образом ворога; Залякування ворога власною силою тощо[14, с. 138].

Основними методами інформації та психологічної війни є пропагандиські настрої, плітки, дії провокаційного характеру, хибна інформація, тиск на психологічний стан, зміна свідомості та інше.

Найпоширенішим методом є пропаганда, яка включає поширення та пояснення будь - яких думок, ідей, навчання, знань.

Роль пропаганди була вперше проаналізована у творах Х. Лассоуелла, що визначало її як особливий тип знаряддя, що має вплив на психічний стан ворога. Серед основних цілей пропаганди автор включає: підбурювання ненависті до ворога; підтримка дружніх стосунків з союзниками; підтримка хороших відносин з нейтральними країнами і, якщо можливо, намагається співпрацювати з ними; ворога деморалізація [15, с. 91].

Цікавим є інтерпретація французького соціолога Дж. Елла, який запропонував розрізнити вертикальну (класичну версію пропаганди, як ми всі уявляємо, надходять зверху вниз з пасивною реакцією аудиторії) та горизонталь (реалізовано в певній соціальній групі і не зверху; в цій ситуації всі учасники рівні, між ними немає лідера, і тому інформація сприймається з максимальною впевненістю) пропаганда.

Автор також розрізняє два типи горизонтальної пропаганди: китайці (члени групи не вимагають висловлювати власну думку) та американську (вона включає діяльність та ідентифікацію індивідуального ставлення людей), спричинених специфіками групової динаміки [Цит. за: 16].

Основні методи пропаганди включають: створення образу жертви у масовій свідомості масової підсудної, яка насправді є злочином, передаючи відповідальність і приписуючи власні злочини супернику, ігноруючи факти та стигматизуючи всіх, хто не погоджується з пропагандою.

Ці методики використовуються РФ під час гібридної війни з Україною, таким чином, визначає методи, що застосовуються під час спеціальних пропагандистських кампаній в Україні: « Побудова довіри в цільовій групі

(використовуючи загальні та встановлені твердження, посилання на владу, цитати тощо.

Ці прийоми використовує Росія під час гібридної війни з Україною. В. Ткач визначає методи проведення спеціальних пропагандистських акцій в Україні: «встановлення довірчих стосунків із цільовою аудиторією, за допомогою загальноприйнятих тверджень, посилань на авторитети; самостійна розумова робота, тобто підготовка та подача матеріалів таким чином, щоб у аудиторії виникло відчуття, що вони прийшли до запропонованих висновків абсолютно самостійно, крім того, для прийняття цього рішення вони провели серйозну розумову роботу; використання образу енциклопедичності автора, який оперує матеріалом й надає противнику звістку [17, с. 104].

Дезінформація та поводження з інформацією В. Петрика досягається за допомогою: тенденції подавати факти (інформуючи, що є тенденцією давати факти чи іншу інформацію про події, що використовують спеціально вибрані правдиві дані; як правило, використовуючи цей метод, спеціально створений інформацією в дозах, до напруги); дезінформація «від протилежного» (у спотвореній формі є інформація про істину або в ситуації, коли їх об’єкт напрямку сприймається як помилкова; в результаті виникає ситуація [18, с. 202].

Диверсифікація громадської думки має на меті розвіяти увагу правлячої еліти держави до різних штучно підкреслених проблем, тим самим відволікаючи її від вирішення пріоритетних завдань соціально-політичного та економічного розвитку, щоб забезпечити нормальне функціонування суспільства та держави . Його форми: дестабілізація ситуації в державі чи її окремих регіонах; посилення кампанії проти політичного обмінного курсу правлячої еліти держави та її окремих представників різними міжнародними установами; Ініціалізація антипоглинальних кампаній та інші скандальні випробування, застосовуючи міжнародні санкції з інших причин [14, с. 139].

Психологічний тиск також є загальним методом впливу на мислення людей. Його заява включає шантаж, загрози переслідування, репресії, вбивства

тощо, надання інформації про реальні або віддалені загрози та небезпеку, терористичні дії та саботажі. У внутрішній практиці телефонний тероризм є найбільш поширеним. Телефонні дзвінки з інформацією про передбачуване пом'якшення громадських місць, залізничних станцій тощо.

Основні технології тиску включають: шахрайство, блеф, політичні ігри та містифікацію, маніпулятивні події, провокації, психологічні та таємні операції, політичні ігри та рекламні кампанії, дезінформація, чутки тощо.

В даний час провокація є одним із найпоширеніших методів війни, який дозволяє опоненту змусити невигідні дії.

Поширення спаму - це спеціальна технологія інформаційної війни. Г. Почепцов зазначає, що відсутність інформації негайно компенсується чутками. Він навіть вказує на можливість існування певного закону щодо можливості вакууму інформації: коли він не надається офіційними джерелами, він негайно з'являється в неофіційних каналах [19, с. 211-216].

Всі перелічені алгоритми психологічної війни використовуються в період інформаційного наступу на Україну. Також служба безпеки встановила, що російські ЗМІ також використовують інші методи впливу на глядача: вони розповсюджуються на половину правди, демонструють детальні сцени вбивства та насильство, намагаючись створити образ противника у свідомості глядачів. [20, с. 269].

1.2. Характеристика правого врегулювання «гібридних воєн» на сучасному етапі, нормативно-правове законодавство щодо протидії «гібридним війнам»

З теоретичної точки зору, важливість диференціації термінологічного та міжнародного права в контексті «гібридної війни», «гібридний конфлікт» може відігравати вирішальну роль у міжнародній кваліфікації цих подій [21, с. 63].

Гіпотетично міжнародна кваліфікація процесів, які називаються «гібридною війною» також створює юридичні передумови для визначення структури правової оцінки реальних подій, обставин, процесів у позиції

«гібридної війни». Впровадження юридичної кваліфікації, а саме: визначення міжнародних стандартів, які можуть підлягати реалізації.

Як результат, міжнародно-правова кваліфікація може створити правові можливості для формування правової оцінки військово-політичної практики гібридних явищ з точки зору загального міжнародного права, міжнародного гуманітарного права та права збройних конфліктів. У зв'язку з цим міжнародно-правовою основою для кваліфікації «гібридна війна»/»гібридний конфлікт» може бути стаття три (g) Резолюції 3314 (XXIX) Генеральної Асамблеї об'єднаних націй. Стаття 3 резюмує, що будь-який із наступних актів, незалежно від того, чи оголошено війну, відповідно до статті 2 вищезгаданої Резолюції, буде кваліфікуватися як акт агресії. [21, с. 110].

Звертаючись до пункту g) статті 3 «Заслання державою чи від імені держави (автор: розуміти «Російська Федерація») озброєних банд, угруповань та регулярних сил або найманців, що здійснюють акти застосування збройної сили проти іншої держави(автор: розуміти проти «України») настільки серйозного характеру, що це дорівнює перерахованим вище актам, або її істотна участь в них»[22, с. 78].

Для того, щоб повністю зрозуміти гібридну війну як стратегічну концепцію, необхідно враховувати існуючий юридичний режим, що регулює застосування сили за міжнародним законодавством. Враховуючи юридичні аспекти гібридного конфлікту, в свою чергу, він вимагає визнання, що деякі дії гібридної операції можна класифікувати як агресію. Це вимагає додаткових теоретичних пояснень для визначення, які гібридні заходи можуть бути кваліфіковані як силові втручання. У питаннях гібридної війни необхідно включити постійний словник міжнародного права.

Не існує єдиного загальновизнаного визначення гібридної війни. Альтернативні назви можуть включати нелінійну війну, активні заходи або конфлікт у «сірої зони». Держава, яка розпочала гібридну війну, досягає мети внутрішньої нестабільності іншої держави, віддаючи перевагу слабким засобам, таким як інформаційні атаки та операції впливу в поєднанні з економічним

тиском, підтримкою місцевих опозиційних груп, дезінформацією та злочинністю. Також використовується таємне розгортання підрозділів у немаркованій формі чи солдатах, які не входять до регулярної армії. У Гібридній війні акцент робиться на інформаційних можливостях та посередникам з лав недержавних акторів.

Стратегічні переваги гібридної війни полягають у тому, що участь стану агресора важко довести. Юридична невизначеність агресора затримує або відволікає реакцію, яка в іншому випадку була б рішучою, включаючи владу, або є міжнародною [23, с. 47].

В останнє десятиліття гібридна війна була пов'язана в основному з агресивною зовнішньою політикою Росії. Розробка та практичне застосування концепції гібридної війни в Росії пов'язана з радником президента Путіна з питань соціально-економічного розвитку та співпраці з державами СНД, Абхазією та Південним Оссетом Суко та начальником генерального штабу Збройних сил Росії, армія Герасим. У 2013 році Герасімов окреслив погляд на гібридну війну як асиметричну реакцію на поширення ліберальної демократії в глобалізованому світі, хоча російські документи, включаючи твори Герасіма, не використовували термін «гібридна війна», а «нелінійна війна» або війна «Війна нового покоління».

Тому основою російської гібридної стратегії є широке використання політичних, економічних, інформаційних, гуманітарних та інших немічних засобів, які будуть використовуватися у зв'язку з рівнем протестів населення, і буде підтримуватися військовими засобами прихованої явища [24, с. 38].

Російське вторгнення в Грузію в 2008 році, анексія Абхазії та Південної Осетії, незаконне тимчасове окупацію Криму в 2014 році, території в Донецьку, Луганську, Харкові є прикладами російської гібридної війни у його класичній формі. Гібридна війна не обов'язково закінчується анексією території. Кампанії дезінформації, підбурювання антиурядових протестів, одна з яких у 2007 році усувала комп'ютерну інфраструктуру Естонії. [25, с. 51].

Гібридні способи війни, що керують війною, поширюються швидко та все більш успішними та порушують територіальну цілісність та політичну незалежність держав під міжнародним захистом. Міжнародне право, яке регулює застосування сили та визначає гібридну агресію, стає ключовим елементом боротьби з гібридною агресією.

Міжнародний воєнний трибунал у Нюрнбергзі в 1946 році визначив агресію як «вищий міжнародний злочин». Агресія поставлена поза законом також Пактом Бріна-Келлога [27, с. 102], воєнним трибуналом в Токіо, заборонена Статутом ООН [28], поправками до Римського статуту Міжнародного кримінального суду [29, с. 41]. Тобто, світ визнав напади як не виконнання міжнародного права.

Однак з Нюрнберзьких процесів не було випадків, коли країна була покарана за вчинення агресії. Держави продовжують не погоджуватися з запропонованими визначеннями агресії та основними державами, які не підписали римський статут - включаючи США, Індію, Китай та Росію - не погоджуються з певним визначенням, прив'язаним до змін та добавок. Тим не менш, агресія запобігає як однобічним, так і множинним. Створення міжнародної коаліції, щоб змусити війська Саддама Хуссейна покинути Кувейт у 1990-1991 роках є ефективним прикладом прояву колективної волі протистояти силою.

Однак гібридна агресія не проводиться у вигляді танкової блискавки та солдатів у національній формі, які заходять за кордон задля захоплення держави - сусіда. Не всі сучасні напади були такі швидкі, як операції «Щит пустелі» (Operation DesertShield)і «Буря в пустелі» (Operation DesertStorm). У випадках, коли акт агресії не відразу очевидний, або коли статус жертви чи агресора не рекомендує силової відповіді, застосовуються непримусові заходи, такі як економічні санкції, дипломатичні ноти про засудження або усні занепокоєння.

Це була відповідь на кроки Росії в Грузії, Криму, Східній Україні, а потім по всій Україні. Було проведено широке міжнародне засудження російської

агресії та загальної підтримки заборони агресії. Міжнародна реакція не призвела до повернення територій, окупованих Росією Джорджією та Україною. Це був один з небагатьох випадків після 1945 року, коли держава насильно змінила свої кордони і анексувала територію іншої держави. Тому дуже важливо включити заходи гібридної війни в існуючу юридичну базу, які агресор намагається обійти. Гібридна війна - це не простий набір ізольованих випадків або набору методик, а загальна стратегія, спрямована на дестабілізацію існуючого конституційного порядку (рис. 1.1).

СФЕРИ ГІБРИДНОЇ ВІЙНИ	Правові аспекти			
	Теорія права	**Міжнародне право**	**Гуманітарне право**	**Конституційне право**
	ПОЛІТИЧНА			
	У державі-мішені, підтримувати етнічне самовизначення, а не державний суверенітет	Підкреслювати змінність норм міжнародного права, заперечувати їх непорушність	Стверджувати, що Росія несе відповідальність за захист своїх співвітчизників у ближньому зарубіжжі	Відстоювати пріоритет конституції Росії перед міжнародним правом
	ДИПЛОМАТИЧНА			
	Підкреслювати право Росії на "сфери інтересів", розмивати кордони між війною і миром	Визнання нелегітимними урядів сусідніх держав, щоб виправдати російські захоплення і приєднання територій	Створити нові етнічні реалії шляхом видачі російських паспортів в інших країнах.	Заявляти, що передача Криму Україні суперечила конституції СРСР
	СОЦІАЛЬНО-КУЛЬТУРНА			
	Використовувати історію для правового обґрунтування гібридної агресії і анексії	Заявляти про домінування російських "сакральних цінностей" над особистими правами людини	Надавати російське громадянство на підставі історичних факторів.	Ліквідувати інститути етнічних меншин; звинуватити їх в пропаганді сепаратизму
	ІНФОРМАЦІЙНА			
	Заявляти про статус Росії як законної спадкоємиці Радянського Союзу, коли це вигідно	Представляти існуючий міжнародний порядок як вигідний Заходу та дискреційний стосовно Росії	Заявляти, що етнічне російська меншина зазнає утисків і їй відмовлено в праві на використання рідної мови	Стверджувати, що відповідно до радянських законів розпад Радянського Союзу був "не конституційним"
	ЕКОНОМІЧНА (ФІНАНСОВА)			
	Створити юридичну основу для домінування в євроазіатській економічній інтеграції	Конфісковувати іноземне майно як компенсацію за російське майно, заморожене західними країнами	Використовувати потік мігрантів в ЄС для тиску на нього	У воєнний час підпорядкувати економічні суб'єкти державним інтересам
	ЕНЕРГЕТИЧНА (ІНФРАСТРУКТУРНА)			
	Заявляти про російський державний суверенітет над енергоресурсами.	Протистояти західним санкціям щодо енергетичної інфраструктури Росії	Руйнувати енергетичну інфраструктуру для виправдання відправки колон з гуманітарною допомогою	Надати право Національній гвардії Росії захищати інфраструктуру
	КІБЕРНЕТИЧНА			
	Заявляти про російський державний суверенітет над кіберпростором	Протистояти санкціям США, введеним за втручання у вибори	Заважати роботі міжнародних організацій з гуманітарної допомоги	Піддати кібератакам виборчі системи країн Заходу
	РОЗВІДУВАЛЬНА			
	Визначити західні правові концепції як такі, що чужорідні та направлені на підрив інтересів Росії	Протистояти західним санкціям у відповідь на застосування хімічної зброї у Великій Британії	Вести збір розвідувальних даних під час заходів примирення	Юридично закріпити пріоритет російських служб безпеки перед правами громадян
	ВІЙСЬКОВА			
	Заявляти про право Росії на попереджувальні дії за кордоном	Відстоювати право на проведення військових навчань за межами російських кордонів без повідомлення	Ускладнювати життя цивільного населення для викликання гуманітарної кризи	Визначити збройні сили Росії як опору внутрішнього порядку в країні

Рис. 1.1. Правові аспекти гібридної війни Росії

Статут ООН [28, с. 113] забороняє агресію, забороняючи використовувати силу без юридичних причин. Стаття 2 (2) 4 гарантує право

держав на свободу від загрози сили або застосування сили проти їх територіальної цілісності та політичної незалежності. Заборонене застосування сили передбачає рівень збройної атаки (хоча для цього рівня не потрібно), на який самозахист виправданий відповідно до статті 51 статуту ООН, а також положення про колективну оборону, що міститься в Стаття 5 Договору про Вашингтон 1949 року.

Незаконне застосування сили в порушення статті 2(4) зазвичай вимагає залучення сил до бойових дій, незалежно від того, чи є вони регулярними збройними силами в традиційному розумінні, чи недержавними військовими групами, як це визначено рішеннями Міжнародного суду ООН, включно з рішенням 1986 року щодо дій США в Нікарагуа та рішенням 2005 року щодо дій Уганди в Демократичній Республіці Конго. Ця юридична рамка показала свою здатність реагувати на зміни в засобах, які використовуються державами для розв'язання війни. Наприклад, у випадку кібер - операцій «Посібник з Таллінна», звіт про застосування існуючого міжнародного права до кіберпростору, складеного міжнародною групою експертів [25, с. 50] підтверджує, що кібер - операції можна вважати незаконним застосуванням сили, якщо вони пов'язані з збройними силами держави або якщо їх наслідки порівнянні з наслідками традиційних звичайних операцій.

Тому, згідно з теорією, що міститься в Хартії ООН, заборона застосування сили може бути застосована до гібридних загроз, якщо вони використовують традиційні війни для знищення або звільнення інфраструктури в гібридній війні. Це руйнування буде таким же, як і від використання активних військових дій.

На практиці гібридні інструменти розроблені, щоб уникнути звинувачень у порушеннях статуту ООН, навіть якщо вони представляють незаконне використання влади. Цього можна досягти різними способами, і одним із них є виконання таємних операцій. Держави давно проводять таємні операції, які, ймовірно, порушують статтю 2 (1). 4, що забороняє втручанню.

Хоча причини таємних дій різні і часто змішані, застосування сили може здійснюватися таким чином, що принаймні частково відповідає міжнародному праву. Відмова у власному провадженні обмежує можливість застосування Thonkiojuris до провадження, що порушує положення Хартії ООН. У контексті гібридної війни такі мотиви не слід враховувати.

Приховані кошти надзвичайно важливі для стратегії гібридної війни не тому, що вони допомагають уникнути відкритого порушення статуту ООН, а тому Держави посіяли насіння сумнівів стосовно відповіді хто це виконав. Інші гібридні заходи просто не враховуються в статуті ООН щодо заборони сили. Тому економічні заходи не вважаються порушенням статті 2 (1). Дезінформація та злочинність також не підпадають під визначення агресії. Однак діяльність, яка не опускається нижче застосування сили, все ще може бути незаконною, оскільки вони представляли б форму втручання. Непроникність суверенітету чітко закріплена в доктрині суверенної рівності, яка закріплена у статті 2 (1). ООН. Генеральна Асамблея ООН висловила свою думку щодо цієї концепції. У заяві 1965 року Генеральна Асамблея визначила втручання як «втручання у здійснення суверенних прав держави» до насильницького повалення уряду.

У заяві, прийнятій у 1970 році, Генеральна Асамблея підкреслила: «Заборона на втручання у внутрішні та зовнішні справи будь - якої держави, а також усі інші форми втручання чи спроби загрожувати державі чи її політичних, економічних та культурних елементах». Під інтервенцією також можна розуміти втручання, яке рідше згадується в міжнародних документах. Ключова фраза міститься у відомому рішенні Міжнародного суду ООН, прийнятому в 1986 році, щодо Нікарагуа.

Суд підтвердив право всіх держав вирішувати питання, що стосуються суверенітету держави, включаючи ті, що стосуються політичної, економічної, соціальної та культурної системи держави, а також визначення її зовнішньої політики. Коли на ці функції держави чиниться тиск, зокрема шляхом підривної діяльності чи непрямого застосування сили, такий тиск вважається незаконним втручанням.

Своєчасність міжнародних питань кваліфікації міжнародного збройного збройного конфлікту гібридного типу також свідчить про симпозіум, організований у Пентагоні, консультанта офісу начальника штабу Збройних сил США, бригадного генерала Річарда Гросса (11 вересня, 2015). Титул симпозіуму – Що таке гібридний конфлікт?

Слід звернути увагу на основні висновки, сформульовані на симпозіумі, а саме: тему обговорення, конфлікти, які містять як елементи конфлікту між державами, чинні закони війни, зрештою, не містять категорії «гібридна війна». У зв'язку з цим прагматична постановка поставлених питань: І чи є потреба якось вирішувати такі конфлікти? [30, с. 4].

У цьому контексті характеризується думка російського експерта В. Котра. Котліар, уповноважений посол, член Комісії з міжнародного права Міністерства закордонних справ Росії, арбітр ООН з міжнародного морського права, пише у статті з питань «гібридної війни». Насправді події в Криму та Донбасі є лише результатом «гібридної війни», який Захід розвів проти уряду Януковича в Україні - і опосередковано проти Росії - з 2012 року та що триває донині». [31, с. 2].

Тобто, роблячи аналіз позиції експерта та його представників російської влади стосовно окупації Криму, який є українським та конфлікту, що мав збройний характер на Донбасі, стає зрозуміла міжнародно-правова аргументація позиції Росії , що стосується початку війни проти України [32, с. 6].

За словами автора прагматизму застосування наукової гіпотези Альберта Ейнштейна, необхідність змінити спосіб мислення у вирішенні отриманих проблем може виконати теоретично - метитологічну детермінанту пошуку альтернативних юридичних оцінок гібридної війни «Гібридної війни «Явище з точки зору сучасного міжнародного права.

Перш за все, принципово інший ієрархічний/вертикальний, а не статичний/горизонтальний рівень юридичного змісту «гібридної війни», відхід від опису подій та процесів, які можуть створити основу для пошуку

правильних відповідей на державу проблеми на практиці потрібна. Основна позиція: який механізм правового регулювання може бути застосований ?

Визначення необхідної умови успішної формулювання збалансованих міжнародних оцінок кваліфікації останніх явищ у практиці міжнародних відносин як «гібридної війни», «гібридна загроза», «гібридний конфлікт», на думку авторів, є застосуванням права Теоретичні та методологічні підходи до аналізу можливих відповідей, які створюють можливість порівняння, засновані на суб'єктивних судженнях експертів у можливостях аналізу набору критеріїв відбору, що визначає логіку аргументації альтернативних можливостей мирної вирішення конфліктів.

Водночас, у контексті застосування на практиці новітніх військово-політичних термінів «гібридна війна»/»гібридний конфлікт», можливого міжнародного судового розгляду міждержавних спорів між Україною та Росією, пріоритетними підходами є критерії міжнар. право загальне, міжнародне гуманітарне право [34, с. 4].

За словами автора, проблема юридичної кваліфікації явища «гібридної війни/конфлікту» не співвідноситься з системою догматичних звичайних нормативних рецептур міжнародного гуманітарного права, правом збройного конфлікту з точки зору сучасного міжнародного права.

Таким чином, проведений аналіз створює підстави для формулювання наступних висновків:

- існують еволюційні зміни в системі міжнародних відносин та підсистемі міжнародного права, в результаті яких існуючий механізм міжнародного регулювання є неефективним у запобіганні та реагуванні на сучасні виклики, загрози збройних конфліктів (приклад: агресія Росії проти України);
- поточні звичайні стандарти та принципи сучасного міжнародного гуманітарне право не відображає останніх змін;
- сучасні міжнародні збройні конфлікти з існуючими елементами «гібридної війни»;

- Росія по суті порушує міжнародні юридичні зобов’язання Російської в міжнародній спільноті
- «Гібридна війна» та «гібридний конфлікт» - це новий тип війни на початку 21 століття. [34, с. 8].

Що стосується міжнародної кваліфікації визначення «гібридної війни», «гібридний конфлікт» - це неіндиціалізований юридичний зв’язок, з регулярними збройними силами, нерегулярними воєнізованими групами, поєднуючи традиційні та нетрадиційні методи, терористичні засоби війни, що деморалізують збройні сили опонента та населення на території державної підрозділу, щоб досягти військової та політичної перемоги над ворогом.

1.3. Аналіз та характеристика найважливіших аспектів «гібридних воєн»

Загалом гібридною війною можна назвати наступні військові дії, які є неофійні та під час яких, інша сторона нападає на державні структури, має постійну армію та основні ворога за допомогою місцевих нападників і сепарів, що підримуються зброєю та матеріальними активами з-за кордону та внутрішніми структурами, олігархами, кіберзлочинністю та іншими організаціями. Як показує практика, такі війни стосуються не лише певних територій, а й на вплив мислення людей, коментуючи експерти з гібридної війни, які є сучасним типом партизанської війни, що поєднує сучасну технологію, традиційну війну та негідні технології, - це форма війни, що передбачає різноманітну композицію, засоби, рівень та природу навчання збройних сил [35, с. 12].

Основні інструменти гібридної війни включають такі інформаційні заходи: засоби військової та політичної дезорієнтації противника; дезінформація власних ресурси. Дії, спрямовані на блок передачі даних з метою створення атмосфери напруги в суспільстві країни від чекання нападів та по всій лінії фронту та впливу на свідомість українців і пошиення паніки [37, с. 2].

Російські ЗМІ, в тому числі акредитовані на Заході, використовувалися для інтенсивної багатоканальної пропаганди та переконання світової спільноти в точках зору, запропонованих російським військово-політичним керівництвом. Серед найвідоміших: Sputnik, Russia Today, Pia Новости, Life News.

За словами Саймона Шустера, глобальна мережа RussiaToday є основною зброєю російської влади в інформаційній боротьбі. Його аудиторія у 2015 році склала 700 мільйонів людей у понад 100 країнах. Бюджет Росії на 2012 рік становив 275 мільйонів євро, а на 2014 рік – уже 500 мільйонів доларів. Станом на 2012 рік цей канал займав перше місце в світі за державними витратами на одного співробітника, які досягли $183 тис. на людину. [38, с. 6].

Як зазначає конгресмен США Дена Майка, з 2014 року Росія заплатила на брехливу пропаганду більше дев'яти мільярдів доларів. На місцевому рівні Росія ще оплачує проросійські ЗМІ.

Постійне збільшення інформаційних потоків унеможливлює їх контроль будь-якою державою. Адже завданням під час протистояння в інформаційній сфері є не контроль над потоком інформації, як слушно зауважує О. Дугін [37, с. 4], а контролювати алгоритм потоку інформації, який він дозволить її дешифрувати і таким чином захистити суспільство та інституції, які ним керують.

Сфера застосування засобів гібридної війни: населення зони конфлікту, населення тилу, міжнародне співтовариство.

Форма ведення даного виду війни:

- заворушення громадськості - акції громадянської непокори, демонстрації, блокади, вуличні сутички,

- повстання - відкриті військові дії проти офіційної влади,

- партизанщина - прихований збройний опір офіційній владі,

- тероризм - організація та вчинення резонансних вбивств, підрив транспортних засобів, будівель, місць масових соціальних контактів (онлайн і офлайн),

- громадянська війна – військові дії між прихильниками різних ідеологічних, територіальних чи національних груп усередині держави [39, с. 12].

Щоб зібрати всю інформацію про військову агресію Росії проти України, яка почалася в 2014 році з анексії Криму, знадобляться багато років. На жаль, окопи гібридної війни відбуваються не лише в Україні. Вони відбуваються по всьому світу, де б ви не були.

За даними Washington Post, у 2014 році російська військова розвідка (ГРУ) створила понад 30 псевдоукраїнських груп і акаунтів у соцмережах, а також 25 «верхових англомовних» видань. Під виглядом звичайних українців оперативники ГРУ фабрикували інформацію та транслювали коментарі, щоб налаштувати проросійськи налаштованих громадян проти протестувальників. У лютому 2017 року міністр оборони Росії визнав наявність у Росії «сил інформаційних операцій».

Аналіз аспектів інформаційної війни та гібридної війни потребує розуміння її дискурсу, який розкриває не лише використання інформаційних технологій та комунікаційну взаємодію, а й концептуальний образ світу тих, хто цей дискурс формує. В контексті українсько-російського конфлікту йдеться насамперед про корекцію ціннісних орієнтацій та політичних інтересів об’єктів впливу. На думку К.С.Серажима, мовлення як відображення процесу орієнтації людини в системі її цінностей, що ґрунтується на системі мовних норм, здійснює ціннісне розчленування дійсності: розкриває категорії «свій – чужий», «свій – чужий», «свій – чужий». формує те, що можна назвати «образом ворога» [38, с. 202]. Новітні технології дозволили більш ефективно формувати образ ворога за допомогою відео, фейкових новин, «розповідей очевидців» та ефекту «присутності». Образ ворога як потужний засіб впливу активно використовувався у протистоянні між Україною та Росією, де активно використовується технологія поширення мемів – спонтанного поширення певної інформації в Інтернеті всіма можливими засобами. Мем (за Ч. Докінзом) як одиниця усної чи іншої культурної інформації має здатність

«розмножуватися» і неконтрольовано поширюватися. Можна сказати, що меми – це своєрідна «мова» нового покоління, яка здатна замінити великі тексти маленькою «картинкою» або маленьким словом. Вони можуть бути патріотичними, як «кіборги», «укропи», або принизливими для ворога, як «ватники», «сепаратисти». «Правий сектор», «візитівка Яроша», «каратели Бандери», «українські націоналісти» – як міфологізований образ «ворога» дозволяють зняти відповідальність за невдачі та продемонструвати власні переваги («духовність», «останній бастіон традиційних цінностей», «православна єдність», «любов братська»).

Характеризуючи компоненти та ознаки інформаційної війни та гібридної війни, слід зазначити, що в їх основі лежить глобальна боротьба ідей – боротьба смислів. В українсько-російській війні – це визнання «русского мира». (з ідеологією відновлення радянської системи) та нової пост майданної України (з новим політичним проектом та постколоніальним синдромом).

Зростання ролі невійськових засобів у досягненні політичних і стратегічних цілей; стирання кордонів між станом війни і миру; пошук союзників серед місцевого населення (прихильників сепаратистських ідей, матеріальних інтересів) та внутрішньої опозиції; неоголошення воєнного стану, приховування присутності своїх військ на окупованій території; формування напруги в суспільстві, паніки, внутрішніх конфліктів, поширення хаосу в структурі інформаційного простору, дестабілізація ситуації в країні – руйнування елементів системи регулювання інформаційної економіки. [44, с. 9].

Цей новий тип війни вимагає інтенсивного захисту та впливу на власний інформаційний простір. Таким чином, сьогодні в Росії значні зусилля присвячені обробці інформації, перш за все для внутрішнього споживача. Вивчення російських засобів масової інформації, що стоїть за завалами «інформації інформації», дозволяє простежити ключові повідомлення пропагандистів, призначених для російської громадськості. Їх суть зводиться до таких тез: «Росія - це велика країна, яка має чудову місію - врятуй людську

цивілізацію від морального декадансу та занепаду», «Росія - це модель духовності, Захід - це світ гріха і розпусти», « «Захід хоче знищити Росію», «всі засоби пристосовані, щоб уповільнити розширення ворожого Заходу, включаючи війну», «всі засоби пристосовані для гальмування розширення ворожого Заходу». Включаючи війну «,» всі росіяни повинні бути виховані в дусі відданості Вітчизни та її збройних силах «,» Криму - це назавжди, і це наша сила «і т. Д. Без жодних сумнівів, такий підхід можна інтерпретувати Як елемент підтвердження - коротких декларацій, що містять психологічні поради, які покращують та стабілізують психологічний -емоційний стан людини чи окремих груп людей, зібраних у громаді. З іншого боку, російські теоретики гібридної інформації та війни (В. Сурков, В. Герасімов) визначили основну загрозу владі Російської федерації як дії потенційних супротивників у інформаційному просторі, направлену на зміну моралі армії та людей Росії. [45, с. 3].

Зауважимо, що військові та пропагандистські дії Росії, незважаючи на їх оманливу суть, мали чіткий та гарний результат для України, адже вони прискорили процес самоорганізації суспільства, самоідентифікації українців та пришвидшення навчального процесу політичної нації. Не менш важливим моментом війни інформації та гібриду початку 21 століття є «документи». Сюжети «Life News» мали на меті не тільки створити «картинку світу» для телевізійної аудиторії, але й сформувати нову «реальність», де було відведе місце «розп’ятим хлопчикам», «західноукраїнським карателям», «натівським військам» та «мужнім ополченцям».

Новини перестали бути джерелом розповсюдження реальних повідомлень, і почали мати виключно власну пропагандистську лінію. Дослідник Р. Гер пише, що «документальний кінотеатр став своєрідним середовищем реальності, де ми можемо змінити порядок фактів, підкреслити деяких і замовкнути інших» [39, с. 392]. Цей підхід дозволяє нам інтерпретувати реальні події та факти, і, перш за все, підтвердити кліше пропаганди реальними «свідченнями» очевидців сцени. Деякі західні та

українські експерти навіть почали говорити про нові 2.0, а також пропаганду 2.0 - ефективний інструмент для маніпулювання інформацією.

Емоціогенність дискурсу такого типу війни обумовлена психомо-емоційним перевантаженням та закликом до емоцій. У цьому контексті необхідно відзначити переважання аудіовізуальної інформації із посиленою емоційною складовою: «Ми бачили розп'ятого хлопчика», «Росія була вражена зрадою братської України», «не було Голодомору -» це трагедія, спільна для всіх народів СРСР «.» Україна хотіла «з'їсти» російський газ і регіон Ростова «,

«Тарас Шевченко - син України, російського громадянина», Новоросія - нова демократична країна» , «Українська армія воює проти» Тихоокеанського російського населення: неповнолітні та фермери, нам потрібна невелика переможна війна «.

Основними інструментами інформаційної та гібридної війни стали Інформаційні заходи як засіб військово-політичної дезорієнтації ворога; дезінформація про власні ресурси; Дії, спрямовані на виведення служби або блокування каналів передачі даних, щоб дезорієнтувати та дезорганізувати, створити клімат напруги в українському суспільстві через постійне очікування страйків та масового наступу на всій лінії фронту та впливу на масову свідомість українців Для того, щоб деморалізувати і сіяти паніку. Однак основні методи залишалися дезінформацією - навмисним розповсюдженням помилкової інформації (неточної, «дозованої»), а також маніпулювання інформацією - спроби змінити свідомість та критичний дух громадськості. [40, с. 4].

Основна програма навчання силовиків Російської Федерації передбачає, що основною формою інформаційної війни є таємна інформація та психологічні операції, які здійснюються шляхом контролю над впливом інформації на свідомість, волю та почуття людини, а Група або маса громадян іншої країни та підриваючи інформаційну інфраструктуру противника.

Об'єкти цього впливу - це не лишень совість, воля та почуття військових та різних сегментів цивільного населення ворога. Цей вплив також повинен

поширюватися на представників системи прийняття рішень у політичних, економічних, соціальних, наукових та технічних галузях, а також у галузі безпеки та оборони країни. Дискредитація дій останнього (правильно чи неправильно) є ефективним методом послаблення ворога. Крім того, на думку російських теоретиків, під час планування заходів щодо впливу інформації, особливу увагу слід приділяти контингенту критичних розуму (радикальних, опозиції, злочинців та всім, хто «ображає» влади) як потенційне джерело загострення кризи у ворожій суспільстві[46, с. 10].

Нинішнє протистояння України та Росії вже давно характеризується оборонним характером, а не наступальними діями української частини, особливо в інформаційному просторі. «Оборонні дії» українських офіційних кіл у формі вибачення: «не бомбардував», «не вбив», «не виконував певних заходів», «не супроводжувались» страйками «симетричними наступами». Цілком ймовірно, що, згідно з прикладом Ізраїлю, Україна використовуватиме фізичне закриття своєї території проти проникнення збройних груп з російської території. Однак, на відміну від фізичного простору, майже неможливо побудувати «стіну» в інформаційному просторі в сучасних умовах.

Аналіз наукових досягнень у цій галузі дає змогу підтвердити, що наукова спільнота, зокрема українська, не приділяє достатньої уваги цій важливій галузі досліджень. Розвиток по суті є науковим, журналістським та освітнім, без більш глибокого аналізу цього явища, його компонентів та соціальних та гуманітарних аспектів інформаційних технологій. У той же час відповідні публікації, в більшості випадків, зводиться до демістифікації помилкових та абсурдних пропагандистських історій (російських ЗМІ) та виявлення проявів масового психозу серед населення. [47, с. 4].

Таким чином, російські пропагандисти знищили «образ світу», створений не лише для власного народу, де українці перестали бути «братами», але вони також змінили масову свідомість українців, які для більшості почали бачити росіян як «нападників», «Молодий брат» в імператорській совісті виявився загадковим і грізним «українським» - є визнанням незалежності України: кінець

колоніального міфу «[40, с. 6]. Але російські експерти з гібридної інформації та війни війни також визначають алгоритми, що тривають у певній кількості країн Європейського Союзу та в певних пострадянських країнах, де створюються структури та одиниці для аналізу та протидії інформаційному простору.

Висновки до розділу 1

Таким чином аналізуючи теоретико-методологічні основи вивчення проблеми «гібридних війн» та дезінформації на сучасному етапі, можна зробити наступні висновки: У процесі розуміння причин та наслідків інформаційної війни слід приділяти особливу увагу на зміну ціннісно-семантичної матриці життєвої структури планетарної спільноти, походження явища мережевих відносин. Це призводить до створення латентного гібридного світу та відповідних форм протистояння у вигляді гібридних конфліктів і навіть гібридних війн. Зміни в природі планетарної системи спричиняють глобалізацію пересічної людини до цілісного бачення соціального світу, розвитку передової колективної свідомості, здатної відображати глобалізацію планетарного життя, можливість подолати помилкове соціальне та індивідуально визначене домінування. Рамка статуту Організації Об'єднаних Націй, принаймні на концептуальному рівні, є достатньою, щоб покласти край гібридній агресії, рівень якої не перевищує класичний поріг для застосування військової сили. Відсутність ясності та лінії поділу, яка виявила втручання агресії, залишила законні прогалини, якими можуть користуватися ті, хто використовує гібридні інструменти. Жоден із інструментів гібридної війни не може вважатися чітким прикладом примусового втручання, якщо ми розглядаємо це як на ізольований інцидент. Однак постійне та скоординоване втручання з метою дестабілізації цільової країни може суперечити положенням статуту ООН, які захищають політичну незалежність держав. Незважаючи на те, що держава з сильними громадянськими інститутами може протистояти повені помилкових звітів, спровокуючи заворушення та стратегічно організовані витоки інформації, спрямовані на підриву виборів, країни зі

слабшими установами можуть не протистояти такому натиску з усіх боків одночасно . Тому важливо, щоб держави та міжнародні та неурядові установи, які прагнуть захистити політичну незалежність, гарантовану діаграмою ООН, розкривають час, проаналізували її та швидко реагувати та координувати, якщо це необхідно. Крім того, тиск повинен відрізнятися від прозорих та законних етапів станів, які вдаються до дипломатичного тиску, який не потрапляє до категорії незаконних перешкод. Збройний конфлікт в Україні затвердив тезу про наявну зміну парадигми війни сьогодення.

Навіть якщо активні бойові дії будуть завершені, Росія продовжуватиме використовувати інформаційні та гібридні методи війни проти України, якщо вона має політичні та економічні ресурси. Пропагандистський дискурс став новим етапом розвитку російської енергетичної системи, де, крім традиційних форм пропаганди та агітації, також використовується новітні інформаційні технології. Нові конотації та підходи до підвищення ефективності впливу з’явилися в дискурсі: «документальний фільм», емоційність та домінування аудіовізуальної інформації. Як показали події українсько-російського протистояння, контроль власного інформаційного простору не менш важливий у присутності сучасної зброї та підготовлених одиниць.

РОЗДІЛ 2
«ГІБРИДНІ ВІЙНИ» ТА ЇХ ВПЛИВ НА НАЦІОНАЛЬНУ БЕЗПЕКУ УКРАЇНИ

2.1. Основні технології «гібридних воєн», що використовуються проти України

Гібридна війна, що спричинена РФ проти України, як вважає Е. Магда, є «існуючий зв'язок просування російської політики на пострадянському просторі», що з приходом до влади В. Путіна була спрямована на підпорядкуванню останньої своїм інтересам. Через те дата початку підготовки до гібридного протистояння досить умовна [62, с. 7].

Проте саме прихід до влади В. Ющенка та перегляд орієнтацій зовнішньої політики Росії з метою відновлення радянського проекту посилило його підготовчу фазу. Він надав приховану та систематичну шкоду жертві, щоб вичерпати свій потенціал, коли прийнято рішення про перехід до гібридного нападу. Важливими елементами підготовки були підготовка та підтримка «п'ятої колонки», використання «м'якої сили», головним елементом якої було вчення про «російський світ», а також військовий, дипломатичний, економічний та політичний. [62, с. 6].

Донецький регіон мав власну регіональну політичну силу - партію регіонів, яка в 2010 р. отримала найбільшу політичну владу держави та під час місцевих виборів загальний контроль регіону: 166 з 180 мандатів помічників. У Регіональній раді, керівні посади у всіх міських радах, районі та селі з корпусом помічників, 24 мерів, міських секретарів у Кіровскі та Сніжне, поодинці містом Горлівка керували безпартійні.

Він формував регіональну ідентичність Донецька навколо минулого, активно спекулюючи на ностальгію «Радянської», одного з найважливіших стовпів радянської політичної культури - боротьби «нашого» проти уявного ворога «фашистів, бандерів» та Прищеплювала масову свідомість комплекс

«переваги» на решту України, зокрема у західних регіонах. Ще одним важливим елементом ідентичності Донецька є Україно-російська бі-етнічність, на яку вплинули тісні зв'язки регіону з Російською федерацією через сімейні зв'язки, торгівлю, загальні кордони та масштабну міграцію донецьких жителів до Росії. Однак, незважаючи на позитивне ставлення місцевого населення щодо сусідньої держави, проросійський рух у регіоні не відігравав значної ролі, а проросійські партії/організації були маргінальними. [63, с. 12].

Непослідовна геополітична політика режиму В. Януковича призвела до соціального та політичного конфронтації на Майдані. Це знищило плани Москви залучити Україну до своїх світових цивілізаційних проектів. Отже, російська частина розпочала заключну фазу підготовки до гібридної війни. Це було кульмінацією використання немічних методів для підготовки збройного нападу. Пізніше, 24 березня 2014 року, редактор -у віці «Kyivpost» К. Горчинська опублікував документ, нібито складений у Раді національної безпеки Російської Федерації під час протистояння Майдану, згідно з якою Кремль націлився використовувати розлади в Україні для захисту своїх інтересів та захоплення більшості регіонів останніх. Він повинен був зіграти одну з найважливіших ролей у цих заходах для юридичної легітимності відповідних етапів. Отже, взимку 2013 - 2014 рр. Відбулася потужна інформаційна операція проти України. Його мета полягала в тому, щоб розвинути конфліктний потенціал українського суспільства, протистоявши жителям південно - східних регіонів та випадків західних регіонів. Слід зазначити, що влада того часу та засоби інформації, яка залежала від неї, також взяла активну частину.

Самоусунення В. Януковича та послаблення центрального уряду прискорили початок гібридної агресії Російської Федерації проти України, що призвело до окупації Кримського півострова та до соціально - політичних розладів у південно - східних регіонах. Цей останній випадок також стався в донецькому регіоні, де представники регіональної партії продовжували

підніматися до місцевого населення, підштовхуючи його до протесту проти нового революційного уряду [65, с. 2].

Перший крок (лютий - 12 квітня 2014 р.) Гібридної війни в донецькому регіоні характеризувався соціально - політичним протистоянням між прихильниками унітарної держави та її опонентів. Пропутінські сили зіграли політичний сценарій у формі «народу заколоту». Місцеві органи влади та члени проросійських організацій прагнули стати його лідерами. Однак вони протистояли один одному. Лідери Донецька прагнули використовувати демонстрації для укладення політичних угод з новим центральним урядом та маріонетками Москви - стати самою владою. Отже, «губернатори народу» та «мера людей» сепаратисти існували паралельно з українською владою. Діяльність декількох центрів впливу на вуличних демонстраціях призвела до розгублених запитів - або відновлення українського закону «про принципи державної мовної політики», і референдум про федералізацію населення південного сходу від обурення коричневої чуми «[63, с. 3].

Після страшних подій на майдані у донецькому регіоні відбулося кілька невеликих мітингів. А саме, у Донецьку, на місці Леніна, сто демонстрантів зібралися, щоб створити «східний фронт» для опонентів нового революційного уряду (фотографія архівів. Мешканці донецька не поспішають приєднатися до «східного фронту») . Цю ініціативу підтримав губернатор регіону, який закликав місцевих лідерів організувати підрозділи само відшкодування, щоб захистити своїх співвітчизників від «правого сектору» та «активістів Майданів». [63, с. 4].

Що призвело до результату чітко зроблених за сценарієм протестів 1 березня 2014 р. у Бахмуті (до 2016 р. - Артемівськ), Горлівці, Єнакієвому, Донецьку, Краматорську, Маріуполі, Слов'янську, прийняли участь майже дві тисячі людей, що протестували. Вони активно впроваджували російські символи й стрічки, що мали георгіївський знак.

Багатолюдний протест стався в Донецьку. Там повинно було бути 2 мітинги: 1 - зроблений органами влади, який спонсорували бюджетники під

назвою «Донбас за закон і порядок», 2 – людьми організації яких мали російські погляди. Але вони об’єдналися. За оцінками, на ньому були присутніми від 5 до 10 тис. осіб. Це було найбільше зібрання так званої російської весни в донецькому регіоні. Його активна група складалася з членів «Республіки Донецьк», Російського блоку та інших антиукаїнських граничних організацій. Під тиском Регіональна рада прийняла резолюцію, яка передбачає референдум про майбутнє Донбасу.

Донецькі сепаратисти систематично пройшли навчання у російських військових таборах, організованих Євразійським міжнародним рухом на чолі з Україножобом О. Дугіним. Там під керівництвом спеціальних служб агресора вони пройшли військову та ідеологічну підготовку. Їх активно підтримували «російські туристи», члени різних російських фашистських організацій, націоналістів та бойовиків, які були мобілізовані різними способами, зокрема через багато груп у соціальних мережах. [66, с. 5].

Крім того, можливість повернення від В. Януковича не виключається, навколо якого представники місцевих органів влади могли об’єднатися. Зрештою, у лідерів Кремля був лист екс-президента, в якому він попросив В. Путіна відправити війська на територію України. Отже, 22 березня 2014 року мітинги на його користь відбулися в певних містах донецького регіону. Наприклад, у Донецьку була прийнята резолюція, в якій «законний президент» був запрошений звернутися до В. Путіна, попросивши його надіслати «російські миротворчі війська» для захисту російського населення регіону. Ці події відбувалися одночасно з офіційною декларацією прем’єр - міністра Росії Д. Медведєва, в якому він підкреслив, що Янукович залишається «законним» президентом. Мабуть, вони розглядали можливість, який повинен бути реалізований у Харкові наприкінці лютого, оскільки, росіяни не виключали можливості лише після уходу Януковича, останнього з цього міста, його нової столиці. Однак він був відхилений через низьку підтримку, з якої екс-президент виграє серед мешканців Донецька та розпад коаліції його колишніх партнерів [65, с. 4].

Успішна окупація Криму «зеленими чоловічками» створила ейфорію серед вищих посадових осіб Російської федерації, російських націоналістів, фашистів та «п'ятій колонці» місцевих щодо можливості повторення сценарію злочинності в Південно - Східні регіони. Однак, на відміну від Криму, в донецькому регіоні офіційна Москва не була готова використовувати свої великі масштабні війська. Це пов'язано з відсутністю російських військових баз у регіоні, а передача збройних сил поза кордоном спричинить непередбачену міжнародну реакцію.

Було вирішено провести спеціальну операцію в південно - східних регіонах, яка згодом була відома як «Російська весна». То, що відбувся сьомого квітня, спровокував захоплення приміщень Регіональної ради та регіонального бюро СБУ в Донецьку для захоплення зброї. Далі було проголошено «Народна Республіка Донецьк». Центр СБУ розпочав антитерористичну операцію для захисту територіальної цілісності держави [65, с. 6].

Під час спеціальної операції офіс СБУ було звільнено, але захват будівлі регіональної ради було призупинено з причин, які не були повністю уточнені. Представники СБУ, розуміючи, що не буде нападу на вилучену установу, почав будувати стабільну ієрархічну терористичну організацію з створенням «тимчасового уряду» та навчанням власних воєнізованих груп. Незважаючи на продовження влади лише для вилучених приміщень, припинення цілеспрямованих спеціальних операцій українських силовиків призвело до накопичення сил «республіки» та до її оволодіння суспільно-політичною, а потім військовою ситуацією в донецькому регіоні .

Другий етап (12 квітня 2014 року) був відзначений проходженням «популярного заколоту» на стадіоні «Збройні конфлікти», який закінчився великим вторгненням у регулярні російські збройні сили в Україні континенталь. Все почалося з військової інтервенції російської підривної групи, «Кримської компанії». Він складався з 52 осіб на чолі з пенсійним офіцером, І. Стрелков («Гіркін»). Його вторгнення з моменту донецька була надана командою «губернатора народу» П. Губарева. Спочатку планувалося взяти

Шахтарську, але після прибуття до України було вирішено вирушити в бік Слов'янську. Їх головна мета, як вважали члени групи, - підготувати відповідні умови для вступу армії [64, с. 12].

Слов'янськ був обраний не випадково. Величезна довжина загального кордону з Росією створила умови, сприятливі для логістики на користь активістів. Це кілька разів підтвердив одним із головних героїв цих подій І. Стрелков, який у своєму відеоінтерв'ю від 6 квітня 2021 року сказав, що «повстання» в Донбасі відбулося через те, що був кордон З поблизу Росії, де можна очікувати допомоги.

Крім того, донецький регіон-це безперервна банда міст, і саме в Слов'янську починається національна дорога Н-20, яка проходить через Краматорську, Дружківка, Костіянтивка, Авдівка, Донецька, Волноваха і закінчується в Маріуполі. Це дозволило їм легко контролювати та передавати активістів між містами. У той час головні центри контролю АТО були розташовані в Харкові, і, отже, українські війська були перерозподілені звідти через місто Ізюм, оскільки регіони Харків і Донецьк були пов'язані одним міжнародним шосе М 03, який пройшов Через Ізюм - Слов'янськ [64, с. 14].

Українська влада, отримавши інформацію про появу «маленьких зелених чоловіків» у Слов'янську, надіслала групу визнання Української служби безпеки для уточнення та перевірки інформації. Але на околиці міста, в селі Семенівна, на нього напали, зазнали втрати солдатів. У відповідь 13 квітня 2014 року Рада з питань національної безпеки та оборони України була змушена почати АТО (Указ Президента України від 14 квітня 2014 № 405/2014 Про рішення Ради національної безпеки і оборони України від 13 квітня 2014 р.) [65, с. 3].

Одночасно на початку збройного конфлікту інформаційна риторика на користь гібридної агресії. Замість «губернаторів та мерів народу» головні герої російських інформаційних ресурсів – міліція. Їх представляють «популярні герої» як «захисники» народу російськомовні проти «фашистів» та «неонацистів» українців. Сили «міліції» були зменшені, а їх база була менш

складена з місцевих співробітників, ніж російські спецнази, націоналістичні волонтери та ветерани війни. Небажання місцевого населення брати зброю та боротьбу кілька разів відзначається основними членами «міліції». Зокрема, ще в 17 травня 2014 року «міністр оборони « та командир «гарнізону». У відеозаписі пан Стрелков зазначив, що на 4,5 мільйонах цього Донецький регіон, лише тисяча людей приєдналися до своїх лав. У вищезгаданому відео інтерв'ю він знову зазначив, що до приїзду регулярних підрозділів російської армії в серпні 2014 року мешканці Донецька не проявляли великого ентузіазму боротися. Подібні думки висловили інші російські волонтери, включаючи членів терористичної групи «Народное ополчение Донбасса» С. Лашин [64, с. 8].

«Народний заколот» не спрацював. Це пояснюється певною кількістю факторів, про які, як ми вже згадували, відсутність російської військової бази на українському континенті, переоцінка проросійських почуттів, продемонстрованих певною кількістю соціологічних досліджень. Серед них необхідно підкреслити опитування Міжнародного інституту соціології Києва «Думки та точки зору жителів регіонів на південний схід від України: квітень 2014 року», а також активний опір мешканців де Донецьк , які організували себе в силах самозахисту, в батальйоні територіальної оборони «Донбас», у координаційному комітеті патріотичних сил Донбасу та інших. Ось чому терористи викликали вогонь крові, щоб створити образ української армії як панікера у масовій свідомості громадян Донецька. Їх основна тактика полягала в використанні місцевого населення як людського щита, встановлюючи свої позиції в містах, у тому числі в житлових районах. З цих позицій вони навмисно розпочали напади проти українських солдатів та артилерійського вогню, щоб нейтралізувати відгуки пожежі, щоб викликати відгуки про цивільні предмети. Один з командирів нерегулярної одиниці «Республіки» нещодавно погрожував знову використовувати ці тактики у випадку військового сходження [77, с. 9].

Продовження військового сходження з використанням важкої зброї - різних гармат ракет та артилерії та численних ракетних установ - збільшило кількість цивільних жертв. Крім того, активісти самих «RPD» навмисно і навмисно бомбили житлові райони, звинувачуючи в українській армії. Згідно з очевидцями цих нападів до Донецька, російські журналісти, як правило, прибувають до початку та негайно показують їх по телебаченню. Подібні випадки траплялися в інших містах донецького регіону. З часом самі активісти почали визнавати певні злочини. Наприклад, командир батальйону «Восток» в інтерв'ю, О. Ходаковський розповів, як його підлеглі бомбардували центр Ясинувата з кількома ракетними установками БМП-21 («Град») [78, с. 22].

Саме в липні-серпня 2014 року - українська армія почала випускати окуповану територію, більшість повідомлень про російські телевізійні канали показали наслідки вибухів, жахливі деталі загибелі цивільних людей, масові страти передбачені «міліції» та «цивільні» українських військ.

Враховуючи професійну, логістичну та кількісну перевагу українських сил безпеки, російські консерватори знали, що це призведе до знищення терористичних груп. Тому вони вирішили підготуватися до вторгнення в регулярні підрозділи російської армії на території України. Основним завданням підготовчої фази було збереження повного контролю над українським кордоном. Військове командування України сформувало відповідні органи командування та контролю - сектори відповідальності (сектори A, C, B, D, M). Сектори A і D відповідали за контроль за кордоном та припиненням постачання незаконної військової підготовки з території Російської Федерації. [77, с. 2].

Одинадцятого липня російська армія розпочала першу атаку ракетами та артилерію проти українських військових позицій у Зеленопіллі з її території. Згодом вона продовжувала свої постійні бомбардування важкою зброєю на прикордонних позиціях, як з території, яку контролюють активісти, так і з моменту власної території. Це призвело до повного оточення української армії в секторі D та блокування маршрутів поставок активістами. Отже, штаб -

квартира АТО вирішила провести операцію з розблокування оточених одиниць. Завдяки успішним діям українських військ на початку серпня їм вдалося зламати вороже оточення та відкликати близько 3000 людей, які були вилучені з сектору та замінені іншими підрозділами. Їх завдання полягало в створенні ізоляційного кола вздовж кордону Станиця Луганська - аеропорт «Луганськ» - Лутугине - Ребрикове - Ровеньки - Дякове - Дмитрівка - Степанівка - Савур-Могила. Таким чином, між територіями, керованими активістами, була створена «буферна зона».

Третій етап (серпень - 5 вересня 2014 року) ознаменував перелом у гібридному нападі Росії проти України, вперше був змушений перейти до традиційного методу війни - збройного вторгнення. Прикордонний контроль дозволив російському командуванню вільно надавати зброю, боєприпаси та активістів з його території, а також розпочати втручання на український континент. Спільна військова операція регулярних російських збройних сил у співпраці з «активістами ДНР» була охрещена «Норд -потік». Московські консерватори внесли зміни між військовими та політичними лідерами «Республіки». Російські громадяни - О. Бородай та І. Стрелков - були відкликані в Російській Федерації в серпні, а місцевий представник О. Захарченко став новим начальником квазі- держави. Отримавши нові повноваження, він оголосив, що нерегулярні одиниці були готові до протидії, який повинен був розпочати через кілька днів. Його оголошення відбулося в контексті офіційної декларації В. Путіна, що Росія надіслала в Україну перший «гуманітарний конвой», який повинен був відправити 280 вантажівок. Ця «допомога» була однією з найважливіших в історії конвоїрів. А 15 серпня начальник на «урядовому засіданні» оголосив про введення резервів «армії Новоросії» у битві: 30 танків, 120 броньованих транспортних засобів та 1200 солдатів, які мали б проходив навчання в Російській Федерації протягом 4 місяців [77, с. 21].

О. Захарченко, був записаний національними та західними журналістами. Вони повідомили про переїзд українського кордону за колонками російських

бронетанкових транспортних засобів, включаючи кілька десятків БМП та вантажівки. Зокрема, близько п’ятдесяти транспортних засобів для бронетанків перейшли на станцію управління, а потім «зникли».

Однак Українське військове командування продовжувало виконання свого плану, незважаючи на його крах, оскільки його головний момент щодо контролю над державним кордоном, щоб запобігти підтримці активістів з російської сторони, не було виконано. Очевидно, що лідери АТО не повністю усвідомлювали високу ступінь ймовірності вторгнення російських збройних сил. Дата втручання останнього в донецькому регіоні все ще є суперечливою через недоступність усіх джерел. Однак, беззаперечні докази їх присутності були отримані 24 серпня, коли бійці 51-ї ОМБ у районі Іловайська взяли в полон 11 псковських десантників 98-ї дивізії [77, с. 24].

Згідно з повідомленнями Генерального штабу ЗСУ, 24 серпня на частину України вторглися вісім батальйонно-тактичних груп, що мали: більше 6 тис. осіб солдатів; більше семи десяти одиниць танків; до 270 одиниць броньованого транспорту.; артсистем - до 90. Це робило загрозу - Маріуполю, Луганську та Іловайську.

Далі були дуже трагічні події через те, що іловайське угруповання, котре було добровольчими батальйонами - було повністю оточене. 26 серпня відбулася запланована зустріч у Мінську в форматі Україна - ЄС - Митний Союз (Білорусь, Казахстан, Росія). Планувалось вирішити три питання під час засідання: виконання Угоди про асоціацію між Україною та ЄС, енергетичною безпекою та стабілізацією ситуації в Донбасі. Однак прес -релізу на цій зустрічі не було. Офіційні декларації учасників лише вказували на спільне розуміння необхідності зупинити сходження збройного конфлікту. Отже, ми все ще не знаємо, що прибули учасники переговорів і що вони погодилися. [80, с. 54].

Відсутність результатів політичних угод призвела до погіршення ситуації українських сил у оточенні. Їх командування в Іловайську вирішило розпочати переговори з російськими представниками на місцях та залишити оточення.

Незважаючи на укладені угоди, випуск «Зелений коридор» закінчився знімком українських колон та величезними втратами.

Цей розвиток змусив двох сторін шукати компроміс. Кремль також зацікавився цим. По - перше, росіяни зазнали значних втрат серед своїх військ, і додаткове перебування в континентальній Україні збільшить докази їх присутності, а по - друге, їм потрібно було структурувати систему управління «Республіки». Крім того, як показали події у вересні серпня, офіційна Москва дуже чутлива до втрат серед своїх військ. Це призвело до активної кампанії, спрямованої на приховування реальних причин їх смерті для національної громадськості, а також відмову захопити Маріуполя, який був вразливим до російських нападів і був захищений лише батальйоном добровольців «Азов».

5 вересня 2014 р. Тристороння контактна група підписали «План мирного врегулювання ситуації на Сході України» або так званий Мінськ-1, в основу якого лягли попередньо запропонований мирний план П. Порошенка та ініціативи В. Путіна.

Четвертий етап (5 вересня 2014 р. - 12 лютого 2015 р.). На цьому етапі головним завданням Москви було сформувати вертикальну силу «Республіки» з повним контролем та порядок неоднорідних нерегулярних груп для формування регулярної військової сили для виживання та стійкості режиму окупації. Зрештою, остання повинна була слугувати прикриттям для присутності російської в Україні, а отже, продемонструвати, що збройний конфлікт був «внутрішнім». «Вибори» від 2 листопада 2014 року, під час яких глава «Республіки» та члени «парламенту» були обрані, закінчили цей процес [66, с. 28].

Підписання Мінських угод не закінчило бойові дії, а призвело до їх розташування. Отже, після підготовки політичних та військових інститутів «Республіки». Кремль продовжував активізувати конфлікт. Основними районами агресії були донецький аеропорт, вказівки Маріуполя та Дебальцеве. Мета полягала в тому, щоб створити ситуацію у вигляді військової поразки українських збройних сил, щоб нав’язати нових умов, сприятливіших для

росіян на тлі військової та політичної деморалізації. З цією метою було обрано місто Дебальцеве, яке було у умовному мішку: з одного боку, воно загрожувало позиціям російських окупаційних військ у Горлівці та Алчевську, а з іншого боку, воно було вразливим до атак на тлі врази з боку нападів на агресор з трьох напрямків [66, с. 31].

Отже, під тиском Російської федерації та політичним тиском західних партнерів, українська частина була змушена підписати «пакет заходів для виконання угод про Мінську» або «Мінський-2». Однак його диспозиції та алгоритм його впровадження містили загрози статусу української держави.

П’ятий етап (лютий 2015 р. - на сьогоднішній день) гібридної війни був відзначений проходженням «гарячої фази» збройного конфлікту до певної ступеня помірної інтенсивності. На цьому етапі українська частина створила глибоку лінію оборони, оснащену потужними укріпленнями, щоб відвернути ворога. Російська частина, з іншого боку, продовжувала використовувати окуповані території як інструмент для дестабілізації внутрішньої ситуації України, щоб підтримувати останню на орбіті її впливу. Ще одним важливим завданням було руйнування українських державних установ з метою демонстрування передбачуваної недієздатності українського народу до будівництва держави.

Для досягнення цих цілей була продовжена розбудова збройних сил «ДНР», які складаються з 1-го армійського корпусу. Ця група підлягала оперативному командуванню 8 -ї армії з комбінованою зброєю південного військового округу Російських збройних сил. А також політичне, ідеологічне та соціально - культурне переформатування матриці окупованої території, щоб відхилити її та поглибити взаємні суперечності та ворожнечі з рештою України. Зважаючи на це, 28 січня 2021 року в Донецьку відбувся міжнародний форум «Російський Донбас», де був представлений політичний документ - вчення «Російська Донбас». Він забезпечує практичні етапи розвитку державної ідеології «Республіки», яка базується на вченнях «Російського світу». Більше того, не існує жодного слова про адгезію цієї території до Російської Федерації,

що вказує на бажання Москви залишити іншу республіку, не визнану на карті. Згодом, 21 квітня 2021 року, був організований ще один форум для обговорення засобів для здійснення цієї доктрини на практиці. У той же час, відео глави «ДНР» передається президенту України щодо переговорів «без лідерів третьої країни». Іншими словами, тактика кремлівських начальників полягає у легалізації своїх ляльок під час міжнародних переговорів, змушуючи українську частину безпосередньо вести переговори з ними і, таким чином, відхиляти всю відповідальність у подіях Донбасу.

2.2. Заходи, які вживає держава, щодо протидії «гібридним війнам» та дезінформації

Безумовно, протидія України «гібридним» загрозам і «гібридній» агресії, яку здійснює Росія, зважаючи на їх масштабність і всеохватність, мала включати комплекс заходів, які також повинні охоплювати усі сфери життєдіяльності країни. Варто зазначити, що залежно від оцінки важливості тієї або іншої сфери, наявності ресурсного забезпечення, фахівців тощо, заходи з протидії, хоч і з різним рівнем інтенсивності, а, відповідно – ефективності, у досить стислі строки були організовані, проводилися та продовжують проводитись. Серед них накладення економічних санкцій проти ряду компаній та осіб Російської Федерації, в тому числі в оборонному секторі, вживає заходів щодо активного протидії нападу та пропаганді російської інформації.

Крім того, не менш важливими заходами стали підписання Україною угоди про асоціацію з ЄС, введення для громадян України права безвізового відвідування значної кількості країн Європи. Активна співпраця України з НАТО, зокрема, отримуючи статус «агресивних країн», зусилля, докладені країнами - партнерами, надати Україну озброєною та не озброєною допомогою, відмовою споживати російський газ, перемогу України в арбітражі Стокгольма над Газові контракти тощо.

Та найбільш помітними стали заходи у військовій сфері [55], [56], [57], [58], [59]. Серед них, насамперед, проведення мобілізації, відновлення армії І зміцнення бойової спроможності держави, встановлення співпраці у військовій галузі з міжнародними партнерами, відновленням національної оборонної промисловості, військовою та військовою технікою із США та НАТО. Стратегічне значення мали і заходи у енергетичному протистоянні з Росією, такі як відмова від закупівлі російського газу, диверсифікація його поставок, протидія створенню газопроводу «Північний потік-2» тощо.

Вкрай важливими стали і зміни у законодавчому просторі, як, наприклад, відмова від «позаблокового» статусу, визнання Росії агресором і покладання на неї відповідальності за людські, матеріальні та фінансові втрати України. Необхідно зазначити, що проблему відсутності правового забезпечення застосування ЗС України в Антитерористичній операції на Сході держави і сьогодні назвати повністю вирішеною за всіма параметрами мабуть буде не коректним.

Із досвіду протидії України військовими засобами «гібридній» агресії з боку Росії Збройні Сили України отримали серйозні уроки. Серед них необхідність своєчасно, вже тільки з появою перших ознак «гібридних» загроз, а ще краще – упереджувально, у превентивному порядку, реагувати на них. При цьому не може визивати сумніву той факт, що форми та способи реагування на «гібридні» загрози також мають бути «гібридними». Це – аксіома! На жаль, у нас такого реагування свого часу просто не було. Очевидно недостатньо його і зараз [55, с. 40].

Загалом, опираючись на набутий Україною досвід протидії російській «гібридній» агресії, можна стверджувати, що основний зміст протидії складають чітке визначення та неухильне дотримання суверенного зовнішньополітичного курсу щодо захисту національних інтересів країни; ведення активної міжнародної співпраці з питань безпеки та конференцій щодо протидії «гібридним» війнам; вступ держави до систем колективного захисту; розробка та впровадження дієвих програм розвитку ЗС України,

інших збройних формувань та правоохоронних органів з урахуванням перспективних напрямів розвитку нових способів збройної боротьби; проведення реформи, на основі якої необхідно створити дієву систему територіальної оборони держави; створення комплексного власного ОПК держави; удосконалення законодавчої бази з питань оборони держави; організація підготовки збройних сил як для ведення сучасних війн і збройних конфліктів, так і участі у спеціальних (стабілізаційних) операціях; визначення принципів комплектування, утримання та чисельності збройних сил, їх достатнє фінансування упродовж тривалого часу тощо.

Отже, протидія України «гібридній» російській агресії – це комплекс політичних, економічних, дипломатичних, інформаційних, соціальних та оборонних заходів, які системно проводяться міжнародною та внутрішньою політикою держави в інтересах нейтралізації можливого воєнного конфлікту між колишньою метрополією та суверенною державою.

Поза сумнівом, основною метою протидії будь-якій агресії, у тому числі і «гібридній», є недопущення руйнування політичної системи держави, захист її суверенітету і територіальної цілісності, забезпечення її економічної та інформаційної безпеки, виявлення правдивої мети конфлікту і способів її досягнення, розкриття для міжнародної спільноти основних форм і методів боротьби у «гібридній» війні. На нашу думку, досягнення зазначеної мети, без вирішення ряду першочергових завдань протидії «гібридній» російській агресії в сучасних умовах, достатньо малоймовірно. Зважаючи на глобальний характер російської «гібридної» агресії, до таких завдань, насамперед, варто віднести необхідність підвищення ефективності протидії міжнародного законодавства різним видам «гібридної» війни, чіткого визначення із союзниками та партнерами, укладення з ними відповідних політичних угод, що мали би дієву юридичну силу, набуття Україною повноправного членства у Євроатлантичній колективній системі безпеки,прийняття дієвої нормативно-правової бази з питань підготовки держави до оборони, протидія впливу противника в інформаційному просторі

держави, досягнення оперативної і технічної сумісності ЗС України зі збройними силами країн-партнерів, створення цілісної системи територіальної оборони держави, прийняття необхідних законодавчих актів щодо посиленого розвитку оборонно-промислового комплексу держави та її сфери національної безпеки і оборони тощо [61, с. 42].

Стосовно протидії російській «гібридній» агресії безпосередньо військовими засобами, на основі набутого Україною досвіду, можливо умовно виділити два основних етапи: перший – з виникненням «гібридної» загрози та другий – безпосередньо з початком «гібридної» агресії (використання регулярних військових формувань). На першому етапі основні зусилля Сил оборони і безпеки доцільно зосереджувати, насамперед, на участі їх у інформаційних кампаніях у межах загальнодержавних заходів протидії (спеціальні операції, акції, окремі заходи, у тому числі у кіберпросторі) з одночасним політичним та ідеологічним тиском на сепаратистські утворення, організації та підтримці руху опору сепаратизму, партизанського руху та підпілля, а також організації і проведення акцій протесту населення на окупованій противником території тощо. Стосовно другого етапу, тобто з початком застосування регулярних військових формувань. Сили оборони держави мають зосереджуватись головним чином на виконанні завдань щодо розгрому незаконних збройних формувань та відновлення контролю над державним кордоном України, веденні бойових дій з обмеженим застосуванням зброї та бойової техніки у тісній взаємодії між усіма їх складовими, а також наданні дієвої допомоги правоохоронним органам з ліквідації терористичних організацій (підпілля), у запобіганні та подоланні наслідків терористичних актів та сприянні у охороні державного кордону України.

Безумовно, основною формою застосування Сил оборони в протидії «гібридній» агресії військовими засобами є, головним чином, збройна боротьба [57, с.141].

Що стосується безпосередньо воєнних, антитерористичних, партизанських і миротворчих дій, то вони, як правило, здійснюються у межах відповідних форм і способів. Узагальнення набутого Україною досвіду протидії російській «гібридній» агресії на Сході держави дає можливість стверджувати, що вибір форми застосування Сил оборони в протидії «гібридній» агресії військовими засобами буде визначатися, насамперед, умовами воєнно-політичної та оперативної обстановки у зоні воєнного конфлікту. Так, основними формами воєнних дій можуть бути операції, бої та бойові дії. Антитерористичні та партизанські дії, залежно від масштабів їх проведення, на оперативному рівні, як правило, будуть реалізовуватись у формах регіональної (зональної) антитерористичної операції або операції об'єднаних сил, а на тактичному рівні – основними формами доцільно мати ізоляційні, охоронні, оборонні, сторожові, пошуково-розвідувальні, пошуково-ударні, патрульні, демонстраційні, штурмові та засадні дії. Миротворчим діям притаманні свої, специфічні та підтверджені світовим досвідом форми застосування військового контингенту, якими є спостереження, патрулювання, конвоювання, супроводження високопосадовців, контроль місцевого населення, гуманітарна допомога населенню тощо.

Стосовно способів застосування військових формувань, варто зазначити, що, відповідно до загальноприйнятих поглядів, спосіб ведення будь-якої форми дій полягає у встановленні певного варіанту вибору напрямів зосередження основних зусиль, послідовності нанесення поразки противнику, побудови форми дій, яка застосовується під час виконання завдань (створення угруповань, оперативної побудови чи бойового порядку, систем розвідки та вогневого ураження), організації управління, всебічного забезпечення тощо.

Важливою складовою протидії російській «гібридній» агресії є і зустрічі у мінському та нормандському форматах. На жаль ефективність мінського формату, на наш погляд, знаходиться на вкрай низькому рівні, і явно не з вини української делегації [77, с. 46].

Отже, розширюється методологія боротьби з гібридними конфліктами, існують різні способи захисту станів від гібридних загроз. Ми спостерігаємо за подіями в різних країнах, щоб захистити різні сфери їхньої країни та глобальної спільноти проти агресивних дій злочинних організацій чи авторитарних режимів, зокрема.

Україна бореться більше року проти гібридної агресії Російської Федерації, але ситуація якимось чином замерзла. З одного боку, вдосконалюється армія, з'являються нові моделі зброї, військові постійно проходять курси, щоб покращити свої навички та оволодіння різним обладнанням, включаючи безпілотники. Навчання з солдатами або іноземними інструкторами постійно проводяться в Україні. Робота знаходиться на дипломатичному рівні.

2.3. Перспективи прогнозування «гібридних воєн» та ефективність протидії дезінформації в майбутньому

Боротьба з дезінформацією та нейтралізація їх негативних наслідків безпосередньо залежить від гарантій свободи вираження поглядів, а також від захисту конфіденційності. Держави спочатку повинні забезпечити, щоб ЗМІ не піддавалися шкідливих втручань і що громадянське суспільство може брати участь у публічних дискусіях без дезінформації, вводячи механізми, щоб відрізнити істину. Посилити неупереджену участь громадян у громадських справах, зокрема на виборах, референдумів тощо. Однак завдання протидії дезінформації ускладнюється тим, що в демократичних суспільствах законодавство свідчить про значну затримку стосовно інновацій, які впроваджують нові технології, через необхідність прийняття рішень консенсусом і, часто, відсутності відповідного технічного досвіду в законодавці.

Зіткнувшись із зростаючим впливом нових технологій на свободу вираження поглядів, Д. Балкін вже зазначив у 2009 році, що «найважливішими рішеннями, що впливають на свободу вираження поглядів, будуть ті, що стосуються технологічних змін, законодавчих та адміністративних правил,

навчання нових комерційних моделей та колективних Діяльність кінцевих користувачів «[41, с. 54].

Сучасний «трикутник» свободи вираження поглядів (національні держави, компанії соціальних медіа та користувачі) був проаналізований Р. Гамільтоном у контексті відповідальності за створення та застосування правил на «Глобальній публічній площі», який дослідник називає сучасні соціальні медіа. Його робота встановлює законні винятки з принципу свободи вираження поглядів з огляду на питання національної безпеки, а також розкривають існуючу практику модерації змісту соціальними медіа, зокрема в рамках боротьби з дезінформацією в контексті захисту Свобода самовираження. Р. Гамільтон пропонує власні підходи до зміцнення боротьби з дезінформацією, зберігаючи свободу вираження поглядів та вільну конкуренцію з цифрової епохи [42, с. 67].

Визначення у законі, законні засоби подолання дезінформації в мережах соціальних медіа в рамках захисту національних інтересів є частиною постійних дискусій у Сполучених Штатах, Україні та інших країнах щодо засобів та повноважень державних органів влади для регулювання відносин що виникає внаслідок використання соціальних мереж. Враховуючи нещодавню поміркованість компаніями соціальних медіа політичного дискурсу в Інтернеті, розрив у законних та внутрішніх правилах безпосередньо впливає на ефективність захисту національних інтересів державність України. Складність проблеми також посилюється еволюцією можливостей дезінформації, спричиненими «глибокими підробленими» технологіями, створеними за допомогою штучного інтелекту.

Навчання юридичних механізмів протидії дезінформації в соціальних медіа в контексті національної безпеки повинно ґрунтуватися на основному конституційному принципі свободи вираження поглядів, за винятком переліку винятків, що гарантують національну безпеку, проводячи виклад загальної декларації людини Права [43, с. 51], з Міжнародного пакту про громадянські та політичні права [44, с. 55] та інші міжнародні юридичні інструменти. Оскільки

соціальні медіа не є традиційними, їхні норми є лише в зародковому стані і змінюються залежно від національних підходів різних держав.

Демократичні держави конституційно гарантують громадянам доступ до інформації та свободу слова, завдяки яким забезпечується безкоштовна та справедлива участь громадян у політичних та інших суспільних процесах.

Американські та українські конституції визнають статтю 19 Міжнародного пакту, що стосується громадянських та політичних прав. Право будь - якої людини на свободу вираження поглядів, включаючи свободу шукати, отримувати та розповсюджувати інформацію та ідеї різного роду, без врахування кордонів, у усній, написаній, друкованій чи художній формі або будь - якими іншими засобами на його вибір , може бути «предметом обмежень, передбачених законодавством, і які необхідні: а) дотримуватися прав чи репутації інших; б) до захисту національної безпеки, з громадського порядку, охорони здоров'я чи моралі «[44, с. 19].

Ця рецептура сприймається майже однаково в українській конституції. Останнє передбачає: «здійснення ... права (на свободу думки та вираження) може бути обмежений законом в інтересах національної безпеки ...» [45, С. 34]. Крім того, Українська конституція передбачає, що «захист суверенітету та територіальної цілісності України, гарантія її ... ІТ - безпека є найважливішими функціями держави, справою всього українського народу» [45, с. 17]. Американська конституція та судова практика недостатньо послідовні у застосуванні та інтерпретації обмежень свободи вираження поглядів. Перша поправка Американської конституції (з точки зору свободи вираження поглядів та преси) стосується лише законів, прийняті Конгресом та місцевими, державними чи федеральними урядовими установами [46], але не до дій приватного засобів масової інформації. Юриспруденція Верховного суду Сполучених Штатів про свободу вираження поглядів у галузі національної безпеки виявила прецедент у вивченні спроби уряду заборонити публікацію класифікованих документів, що стосуються війни у В'єтнамі [47, с. 39] і, хоча

суд відхилив цю спробу, більшість суддів погодилися, що за певних обставин попереднє обмеження публікації може бути конституційним [48, с. 53].

Важливість свободи вираження поглядів для американського законодавства, політики та культури може бути підтверджена формулюванням спільного вивчення кількох американських урядових установ про оцінку загрози насильницького екстремізму інтер'єру походження, який (іспит) не оцінює Дії осіб, що проводяться лише у діяльності, захищеній Першою поправкою (Американської конституції - доданої автором) або інших прав згідно з американською конституцією «[49]. Цей приклад показує, як юридичні норми свободи думки та вираження в Сполучених Штатах, в тому числі щодо заяв в Інтернеті, є життєво важливим, але іноді занадто чутливим для захисту громадського порядку та інтересів національної безпеки.

Таким чином, порівняно з американським урядом, Український уряд має більш широкі конституційні умови для захисту інтересів національної безпеки, включаючи тимчасові обмеження на фундаментальну свободу вираження поглядів. І враховуючи агресію Російської федерації, яка використовує руйнівні дії в кіберпросторі та інформаційних та психологічних операціях, у тому числі в соціальних мережах, можливість регулювати заходи, спрямовані на протидію дезінформації.

Немає сумнівів, що дезінформаційні кампанії підривають демократичні процеси, але як в Україні, так і в Сполучених Штатах, повинні відбуватися публічні дебати щодо передумови щодо обмеження свободи думки та вираження в інтересах національної безпеки та про формування прозорого юридичного механізму застосування закону у кожному випадку.

Сьогодні ці механізми, безумовно, будуть різними для України та США, враховуючи різні підходи до обмеження свободи вираження поглядів в інтересах національної безпеки в правових системах двох країн. На кінцеві рішення, прийняті в США, щодо заходів щодо боротьби з дезінформацією (у тому числі в окремих державах) в соціальних мережах впливають міжнародні аспекти. Так, наприклад, у США відбувається дискусія стосовно судового

рішення Суду ЄС (European Court of Justice) Шремс II (Schrems II), яким визнано недійсним «Щит конфіденційності приватних даних» між ЄС та США (Privacy Shield Decision). Крім того, транснаціональні соціальні мережі передбачають можливість введення шифрування даних, що унеможливлює не лише боротьбу з дезінформацією, але й боротьби з злочином проти неповнолітніх, терористичних демонстрацій тощо. Нарешті, юридичний підхід Сполучених Штатів та інших демократій щодо ГДК в даний час базується в основному на саморегуляції їх діяльності в контексті політики щодо обробки даних та використання послуг [61, с. 21].

Іншим складним юридичним питанням є відповідальність СКМ у контексті свободи вираження поглядів та законодавства, що застосовується до розбіжностей дезінформації.

Чим більше користувачів звертають увагу на платформи соціальних медіа, тим більше доходів від реклами може бути створено. Звіти про дезінформацію часто є більш письмовими, ніж інформація, перевірена фактами, що може заохотити ЗМІ отримати користь від розповсюдження помилкових звітів, що не визначається законом і визначається як незаконна інформація. Як справедливо зазначає пан Амморі, держави повинні встановити «важливість технологічних компаній у контексті свободи вираження поглядів» [50, с. 89]. Отже, майбутні норми щодо боротьби з дезінформацією в соціальних мережах повинні враховувати міжнародні вимоги до прав людини, національні інтереси, а також торгові процеси MSC. Держави завжди мають унікальне право гарантувати основні свободи осіб та компанії та регулювати юридичні дії, спрямовані на обмеження їх відповідно до інтересів національної безпеки.

Зрештою, проблема юрисдикції даних, яка активно обговорюється в контексті кіберіндінгів, також важлива для активації юридичних алгоритмів, спрямованих на протидію дезінформації в мережах. На початку 2000 року Google підрахував, що основою компетентності було розташування сервера, на якому зберігалися дані [51, с. 91]. Однак Д. Даскал встановив, що «настав час перемістити увагу розташування даних до місця розташування та

національності цілі нападу, щоб визначити компетентність поліції за даними» [52, с. 37]. Так само акцент повинен бути зроблений на «орієнтації змісту» SMS дезінформації для концепції компетентності влади української держави.

Тому є можливості працювати в Україні для протидії дезінформації. Згідно з тимчасовим стратегічним настановою щодо безпеки Сполучених Штатів, останні «працюватимуть зі своїми союзниками та партнерами, щоб зіткнутися з новими загрозами демократії, будь то транскордонні атаки, кібер - атаки, дезінформація, дезінформація, дезінформація, дезінформація, дезінформація, дезінформація, дезінформація, дезінформація, дезінформація, цифровий авторитаризм, інфраструктура або енергетичний примус «[53, с. 55]. Двосторонній кібернетичний діалог між США та Україною є основою глобальних зусиль для боротьби з дезінформацією. Як визначено у законі про співпрацю в кібербезпеці в Україні, американська політика полягає у «вдосконаленні здатності України реагувати на дезінформацію та пропагандистські зусилля, що підтримуються Росією в кіберпросторі та через соціальні медіа та інші ЗМІ». [54, с. 12].

Висновки до розділу 2

Отже, досліджуючи «гібридні війни» та їх вплив на національну безпеку України, можна зробити наступні висновки: причиною гібридної агресії Росії стало його зусилля залучити Україну до своїх дій пропаганди. Проте Україна шукала геополітичний вектор свого державного розвитку, що й спричинило призвело майдан. Розклад подій змусив РФ почати агресію зі зброєю. Це закінчилось анексією Криму та заворушень у Донецьку та регіоні, натхненні силами про путінської брехні, які призвели до збройної агресії. Метою агресора було - мати політичний контроль над Україною. Тобто, ситуація весь час змінювалася - масові сутички з переросли у справжні бойові дії, це зумовило Україну виконати контрнаступ. Далі, це спровокувало військове вторгнення російської армії. Воно мало перешкодити розгрому «ДНР». Досягнувши цієї мети, Кремль продовжував посилити конфлікт, щоб накласти свої умови для

вирішення ситуації в донецькому регіоні. Таким чином, було підписано договір, статті якого більше відповідали інтересам Кремля, ніж Україна. На останньому етапі офіційна Москва намагається змінити політичне, ідеологічне та соціально - культурне сприйняття окупованої території, щоб утримати Україну на її геополітичній орбіті через лялькову «Республіку».

Підводячи підсумок, слід зазначити, що аналіз надав документи для наступних висновків щодо створення юридичних механізмів для боротьби з дезінформацією в соціальних мережах у контексті побудови потенціалу боротьби з дезінформацією. Боротьба з дезінформаційними кампаніями з причин національної безпеки вимагає поєднання зусиль Центру з національними суб'єктами кібербезпеки, а також регуляторними органами ЗМІ, стратегічними комунікаційними підрозділами державних органів України у тісній співпраці з приватним сектором, особливо з засобами масової інформації та громадянським суспільством. Створення юридичних механізмів боротьби з дезінформацією в соціальних медіа в контексті національної безпеки повинно ґрунтуватися на конституційних принципах свободи думки та вираження поглядів з ексклюзивним переліком їх можливих обмежень у соціальних медіа для забезпечення національної безпеки. Відповідні юридичні механізми будуть змінюватися в Україні та США через інший підхід до обмеження свободи вираження поглядів в інтересах національної безпеки. Різниця між юридичними та внутрішніми правилами, що регулюють діяльність організацій громадянського суспільства, безпосередньо впливає на ефективність захисту національних інтересів США та України. Немає стандарти, що зв'язують першу поправку до Конституції США для приватних організацій, визначають медіа орієнтацію на прибуток, хоча, наприклад, Facebook та Google, наприклад, встановлюють відповідність принципам свободи вираження поглядів. Агресія Російської Федерації оновлює необхідність зміцнення заходів для боротьби з дезінформацією в Україні.

РОЗДІЛ 3
ДЕЗІНФОРМАЦІЯ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

3.1. Визначення основних понять «дезінформація» та «пропаганда»

У XXI ст. Інформація стала ключовим інструментом для національної влади і перетворила вплив недержавних суб'єктів. В останні роки спостерігається швидкий розвиток дезінформації та пропаганди у всьому світі. Противники використовують пропаганду та дезінформацію для маніпулювання громадською думкою, знищення соціальних та політичних інститутів і, таким чином, послаблюють демократію. Краще розуміння інформаційного середовища, його впливу на геополітичні події та поведінка людини є важливим для підтримки безпеки та прийняття важливих політичних рішень. Основним викликом сучасного суспільства є захист демократичних процесів та людей від вторгнення дезінформації та пропаганди.

Дезінформація – неправдива або оманлива інформація, яка поширюється цілеспрямовано та з метою ввести в оману [62, с. 78].

Мета дезінформації – завдати економічної шкоди, маніпулювати громадською думкою. Дезінформація супроводжується фальсифікованими, поза - контрольними та маніпулятивними зображеннями чи відео. Основними каналами розповсюдження дезінформації є Інтернет - форуми, інформаційні сайти та соціальні мережі. [62, с. 79].

Слід зазначити, що Україна вперше визнала загрозу дезінформації в 2014 році, коли Росія посилила її на українській території. Кампанії дезінформації, зокрема, проводяться третім країнами, найчастіше реєструються в контексті гібридної війни, яка включає кібератакти та злому мереж.

Інформація Erroned - це інформація, яка є помилковою, але створена без наміру шкодити. Найчастіше цей тип інформації використовує мимовільні

помилки, невірні легенди фотографій чи відео, помилкові дати/статистику тощо.

Дезінформація (dis-information) - помилкова інформація, яка була навмисно створена з наміром шкоди. Тобто, це аудіовізуальний вміст, виготовлений або добровільно змінений, спеціально створений для різних теорій змови чи чуток[59, с. 29].

Шкідлива інформація (mal-information) – Інформація, заснована на реальних та використаних фактах, щоб завдати шкоди людині, організації, країні. Це навмисне розкриття особистої інформації в особистих інтересах, навмисна зміна в контексті публікацій.

Отже, Відмінними характеристиками цих визначень є помилковість інформації, наміру та типу пошкоджень. Крім того, ця концептуальна рамка, запропонована авторами дослідження, використовується різними вченими та державними установами. Згідно з цим звітом, інформаційний розлад має 3 фази: створення повідомлень. Лікування - Повідомлення перетворюється на медіа -продукт.

Великою загрозою сучасному суспільству є пропаганда. Поняття з’явилось в 1622 році, але суть набула негативного значення у 20 столітті, коли Радянський Союз та уряд Німеччини на чолі з Гітлером розповсюджували пропаганду відповідно до положень нацизму та комунізму, що створили негативні наслідки. Дослідники Г. Джовет (G. Jovet) та В. О’Доннел (V. O’Donnell) у своїй книзі «Пропаганда та переконання» (Propaganda and persuasion) пропаганда як «навмисні та систематичні зусилля для маніпулювання, сприйняттям форми та керування поведінкою у напрямку, який бажає пропагандист». Пропаганда передбачає заплановане використання будь - якої форми спілкування, призначеної для впливу на дух, емоції та дії групи для конкретної мети».

Модель пропаганди показує, як інформація та переконання можуть міститись у пропагандистській комунікації. Крім того, пропаганда впливає на громадську думку та змінює поведінку громадян. Термін «пропаганда»

пов’язаний з контролем і вважається навмисною спробою змінити або підтримувати баланс сил, що сприятливо для пропагандиста. Загалом ці зусилля пов’язані з ідеологією та чіткою інституційною метою. Отже, мета пропаганди - передати певну ідеологію аудиторії з певною метою[60, с. 774].

Пропаганда налічує декілька форм. Залежно від мети, є позитивна пропаганда та негативна пропаганда. «Мета позитивної пропаганди - сприяти соціальній гармонії та навчати людей у дусі загальновизнаних цінностей. У суспільстві це виконує позитивну функцію пропаганди, інформації та освіти. Основні характеристики такі:

- робиться на користь тих, кому адресована;
- не вробить обману та приховування фактів;
- не містить мети маніпулювання» [60, 775].

Відповідно, Мета негативної пропаганди - нав’язувати певні думки та переконання людям, щоб заохочувати соціальну ненависть, спровокувати протиріччя в суспільстві тощо. Це дозволяє людям піддаватись людям і змушувати їх підкорятися пропагандистам. Є також біла, чорна та сіра пропаганда. При використанні білої пропаганди можна визначити надійне джерело, а інформація надійна та перевірена. Цей тип пропаганди намагається здобути довіру громадськості, оскільки це може бути корисним у майбутньому. Використовуючи чорну пропаганду, джерело інформації прихована та помилкова інформація, чутки тощо. транслюються. Успіх такого типу пропаганди залежить від громадськості та її бажання довіряти джерелу інформації та її змісту. Основна роль відіграє правильний вибір цільової аудиторії та відповідну презентацію інформації в соціальних, культурних та політичних рамках.

Сіра пропаганда знаходиться між білою пропагандою та чорною пропагандою, що означає, що джерело інформації та її змісту не можна визначити з точністю. В основному він використовується для зміцнення обману або для заплутаного ворога чи конкурента. Сіра пропаганда дуже поширена,

оскільки вона включає спотворені документи, статистичні звіти, рекламу [57, с. 8].

Отже, Поняття дезінформації та пропаганди мають загальні та чіткі характеристики. Поширена характеристика цих понять полягає в тому, що вони добровільно поширюють інформацію з певною метою. Відмінними характеристиками є те, що дезінформація виключно орієнтована на руйнівні наслідки, тоді як пропаганда завжди може бути конструктивною. В Україні загальна термінологія «дезінформації», «пропаганда», «фальшиві новини» створює проблему, оскільки немає загальних визначень цих понять, що використовуються в Україні. Поняття «фальшиві новини» можна інтерпретувати по -різному. Проблема дезінформації є багатогранною, і деякі її форми з'явилися після розвитку соціальних мереж. Вони також пов'язані з більш широкими політичними, соціальними та суспільними питаннями. По - перше, політичні суб'єкти часто є дезінформаційними мовниками. Це можуть бути як закордонні уряди, так і національні групи, які активно працюють над тим, щоб підірвати цілісність європейських ЗМІ та політичних процесів. По - друге, не всі ЗМІ відповідають професійним стандартам та незалежності редакції, що сприяє розвитку проблем дезінформації та послаблює довіру європейських громадян у ЗМІ. По - третє, роль цифрових медіа, а саме американських соціальних мереж, які пропонують багато можливостей та послуг комунікації. Інструменти, які вони надають, надають владу громадянам європейським, створюючи нові способи розповсюдження та отримання різної інформації та точок зору з різних джерел. Однак це має свої наслідки, зокрема, створення та розповсюдження дезінформації великого масштабу.

Таким чином, Загрози, що виникають шляхом дезінформації, є частиною розвиваючої складної системи, яка підкреслює важливість спільних зусиль для того, щоб зробити цифрові медіа та соціальні мережі більш зрозумілими та прозорішими для європейських громадян. Зокрема, концепція «дезінформації» визначається блідою як «помилковий зміст, який створюється та розповсюджується для економічної вигоди або навмисно обдурити

громадськість, і який може спричинити упередження для громадськості» [57, с. 12]. Термін «іноземне втручання» підкреслює намір актора втручатися в права людини на політичну свободу вираження поглядів та демократичні процеси іншої країни [57, с. 13].

Здебільшого дезінформація поширюється російськими інформаційними ЗМІ, які поширюються в країнах ЄС, таких як RT та Sputnik. Їх початковою метою було покращити імідж Росії за кордоном, але вони не досягли успіху. Згодом Кремль наказав цим ЗМІ змінити свій підхід до негативного підходу, тобто вони використовувались для приниження образу ворога. Таким чином, Кремль не створює стільки криз, як використовує існуючі вразливості, розбіжності громадян та напружену політичну ситуацію країни [57, с. 22].

Окрім підтримки та вдосконалення свого іміджу, Пекін розробляє інструменти для впливу та втручання з образливими намірами. У Китаї пропагандистське створення є однією з головних цілей Комуністичної партії Китаю (КПК). Партія має велику бюрократичну структуру контролю інформації, яка зараз адаптована до статусу Китаю на міжнародній сцені. Зусилля, докладені на ідеологічному фронті, мають дві цілі: формувати внутрішній політичний простір та підтримати легітимність партії (за цензурою та дезінформацією); Вплив на міжнародну думку та проведіть «інформаційну війну» на користь китайських інтересів.

Органи пропаганди, тобто центральний департамент пропаганди, розташовані на вершині політичної ієрархії. Китайська пропаганда є важливим елементом його публічної дипломатії. Пекін керує змістом і використовує певну кількість засобів для розробки своїх гасел, які мають на меті підживлювати інтелектуальні дискусії щодо Китаю та розповсюджувати позитивну інформацію для громадськості.

Характеристики сучасного інформаційного середовища на платформах соціальних медіа такі:

- Об’ємна кількість даних про людей та їх соціальну поведінку, ті дані які ми залишаємо в Інтернеті, коли ми взаємодіємо з технологіями та

вмістом. Ці дані використовуються платформами для створення детальних оглядів, яких ми є споживачами, громадянами чи потенційними виборцями. Колекція, агрегація та використання даних дозволяють іноземним опонентам орієнтуватися на користувачів з політичною рекламою під час виборів. Ці повідомлення можуть стимулювати підтримку та мобілізацію для певного кандидата або усунути політичну участь певних сегментів населення.

- Платформи застосовують алгоритми - або автоматизовані правила правил чи інструкцій - для перетворення даних у бажаний результат. Використовуючи математичні формули, алгоритми оцінюють, класифікують, організовують та поширюють вміст на основі таких факторів, як особисті дані та уподобання індивідуального користувача, загальні тенденції інтересів та поведінки подібного користувача тощо. За допомогою алгоритмів модерація вмісту впливає на те, як новини та інформація надають пріоритет та показують користувачам різні точки зору або зміцнюють існуючі точки зору, підштовхують користувачів до помилкової та оманливої інформації, або виділяють сенсаційний зміст роботи інші автори.
- Анонімність, тобто платформи пропонують різні види анонімності [59, с. 44].

Той факт, що користувачі повинні використовувати своє справжнє ім’я, впливає на той факт, що боти, тролі або навіть іноземні державні суб’єкти використовують анонімність, щоб приховати свою ідентичність, переслідування або загрозу політичних активістів та журналістів, або спотворити справжні розмови про політику. З анонімністю існує відсутність прозорості щодо джерела інформації та про те, чи є новини, коментарі чи дискусії з справжніх голосів чи людей, які намагаються спотворити публічну сферу. Automation, яка дозволяє обліковим записам публікувати, ділитися або автоматично взаємодіяти з публікаціями або користувачами в Інтернеті. На відміну від людського користувача, автоматизовані облікові записи, які іноді

називають «політичними роботами» або «обліковими записами підсилювача», можуть публікувати повідомлення набагато частіше та регулярно, ніж будь - який користувач. Якщо існує багато способів класифікації автоматизованих облікових записів та заходів, вони, як правило, виконують дві функції, коли мова йде про операції з іноземним впливом.

Автоматизовані облікові записи можуть створити помилкове відчуття популярності, імпульсу чи актуальності навколо людини чи певної ідеї, люблячи, відпочиваючи або обмінюючись інформацією. Наприклад, зомбі - мережі можна використовувати для спотворення онлайн - розмов та розповсюдження помилкової інформації або пропаганди. Автоматизація була неймовірно потужним інструментом для цькування журналістів та активістів, затоплення людей загрозами та ненавистю через рахунки, які навіть не є реальними. [58, с. 185].

Отже, Основні канали трансляції дезінформації такі: прес - агентства або канали громадського телебачення; державні та недержавні установи; Інтернет - медіа та соціальні мережі. Окрім термінів «дезінформація» та «пропаганда», широко використовується термін «історія», що означає історію, інтерпретацію подій. Ворожі історії орієнтуються на почуття, емоції та впливають на певні соціальні вразливості. Вони складаються з справжньої та неправдивої інформації, де історія фактів важливіша за самі факти. Різні історії можуть навіть суперечити собі, оскільки вони стосуються різних груп населення. В основному, ворожі історії базуються на соціальних питаннях і поширюються на різних платформах для підвищення вірусності повідомлення. У світі, перевантаженому інформацією, «помилкові історії» створюються для привернення уваги. Люди, які постійно стикаються з великою кількістю інформації, як правило, довіряють думкам, створеним групам, які підтверджують їхні існуючі переконання. Цей «ілюзорний ефект істини» - це механізм, який надає довіру історіям через попереднє висвітлення, незважаючи на низький глобальний рівень правдоподібності. Повторення збільшує простоту декларації обробки, що дозволяє визначити точність інформації [58, с. 186].

З огляду на вищезазначене, додамо, що дезінформація й пропаганда є міжнародною проблемою та загрозою для середовища людей. Дезінформація створює плутанину та недовіру та зменшує довіру людей до інститутів, які мають вирішальне значення для функціонування здорової демократії, таких як уряд, засоби масової інформації тощо. Це компрометує здатність громадян ефективно брати участь у суспільстві шляхом голосування та іншої громадянської діяльності.

Дезінформація змушує людей приймати рішення, які мають негативні наслідки щодо здоров'я та безпеки людей та фінансового становища компанії. Всесвітня павутина та засоби масової інформації - це сучасні механізми маніпулювання інформацією, які дозволяють використовувати нові інструменти передачі інформації та впливати на настрій суспільства. Тому Інтернет - це середовище, що сприяє поширенню помилкової інформації та пропаганди. Дезінформація та пропаганда настільки ефективні, що вони обманюють звичайних громадян, а алгоритми платформи швидко транслюють помилкові великі розповіді. У інформаційному середовищі, що характеризується надмірна кількість вмісту та алгоритмів, розроблених для збільшення кількості поглядів та відпочинку, ворожі історії можуть швидко стати вірусними, використовуючи особисті забобони. Україна є об'єктом дезінформації, впливу та іноземних втручань. А відповідь більшості західних країн була фрагментарною та повільною, обмеженою юридичними обмеженнями та бюрократією, а також відсутністю реального політичного розуміння проблеми та доказів впливу.

Супротивниками є держави, організації та окремі особи. Вони розробили добре встановлені методології та заклали основи для створення мереж та розповсюдження історій для залучення більшої кількості прихильників для поточних та майбутніх кампаній дезінформації. У Україні важливо швидко реагувати та протистояти цим загрозам. Це ми бачимо в численних документах, основна діяльність яких полягає у виявленні та протистоянні дезінформації та пропаганді.

3.2. Деструктивний інформаційний вплив в українському інформаційному просторі. Виклики та загрози

Наразі прогрес потоку інформації значно вплинув на спілкування між людьми, їх сприйняття світу, взаємодію та доступ до цієї інформації. Завдяки різним програмам та соціальними мережами люди отримують велику кількість інформації в режимі реального часу. У той же час, часові та космічні бар'єри зникли, і більше немає перешкод для вивчення новин з різних куточків світу. З іншого боку, з розвитком нових технологій люди стають більш вразливими до сприйняття інформації. У сучасному світі, де вміст створюється та миттєво розповсюджується на різних Інтернет - платформах, здатність визначати пріоритети різних повідомлень, які представляють ризик репутації та знань громадськості, тепер є головним викликом для професіоналів комунікацій. Зокрема, важливість полягає у здатності ідентифікувати та зрозуміти справжню природу цього змісту. Тому спочатку необхідно визначити концепцію помилкової інформації в загальному сенсі [5, с. 188].

Проблема дезінформації та помилки є багатогранною та відповідною для України. Завдяки появі нових цифрових медіа з'явилися нові форми дезінформації. Перш за все, це пов'язано з політичними та соціальними проблемами та регламентами ЗМІ. Перехід до цифрового середовища пропонує українським громадянам багато нових способів висловити себе, а також знайти та отримати доступ до широкого спектру інформації. З іншого боку, це збільшує кількість інформації, що циркулює в Інтернеті. Тому суспільству важко відрізнити правду від брехні. Отже, ризики дезінформації збільшуються, що значно загрожує демократичним процесам, національній безпеці та соціальній структурі.

Основними причинами розповсюдження великої кількості дезінформації є:

- вільний доступ до Інтернету;
- соціальні мережі;
- оперативність розповсюдження інформації;

- погіршення компетентності в роботі журналістів;
- відсутність юридичної відповідальності за контент користувачів;
- перевантаження інформацією сприяє поширенню дезінформації, оскільки така перенасиченість призводить до зниження концентрації, що значно послаблює людську пильність й здатність виробляти контраргументи [59, с. 112].

Враховуючи вищезгадані причини розповсюдження помилкової інформації на різних платформах, можна сказати, що в сучасних умовах Інтернет почав використовуватись як інструмент для маніпуляції та психологічного впливу на суспільство, а також джерело пропаганди та мовлення помилкової інформації.

В даний час під час війни в Україні найбільше поширені нові політики. Важливим фактором є їх новинка, оскільки вона привертає увагу людей, сприяє прийняттю продуктивних рішень та заохочує обмін інформацією. У цьому контексті виявилося, що помилкові новини сприймаються як останні, ніж реальні. Однак твердження про те, що боти, тобто автоматизовані програми, прискорили розповсюдження реальних та помилкових новин, виявилося помилковим. Саме люди відповідають за швидке розповсюдження помилкових новин.

Поняття «фейк або фейкова інформація» є відносно новим. Адже саме поняття «фейкові новини» почало широко використовуватись з початку XX ст. Протягом багатьох років ця концепція значно розвивалася, «фальшиві новини» використовувались для позначення всього: дезінформація, висвітлення подій у сприятливому світлі, теорії змови та відносини, які читачі/глядачі не цінують, і велика кількість Таким чином, його значення утворилися, що призвело до значної плутанини.

Загалом, термін «фальшиві новини» слід розуміти як навмисне розповсюдження помилкової інформації в традиційних ЗМІ та соціальних медіа, щоб ввести в оману, а також для фінансових чи політичних вигод. Щоб

створити помилкову інформацію, ми використовуємо вигадані історії, фотографії та відео, зроблені в соціальних мережах, новини в ЗМІ тощо[59, с. 115].

Важливо відзначити, існують 4 основні типи фейкової інформації:

- пародія, тобто йдеться про різні новинні сайти, які публікують фальшиві новини для того, щоб висміяти засоби масової інформації.
- Оманливі новини, які певним чином є правдивими, але використовуються в неправильному контексті, тобто за основу беруться вибірково підібрані реальні факти, які згодом потрапляють в заголовки, проте, як правило, є неправильною інтерпретацією наукових досліджень.
- Недобросовісні репортажі, що відповідають порядку денному – це частково правдиві новини, які не повністю перевірені та використовуються для підтримки певної точки зору або позиції.
- Новини, що навмисно вводять в оману, тобто це інформація, яка навмисно сфабрикована з метою отримання прибутків або викликати невдоволення чи плутанину серед суспільства. В даному випадку, здебільшого застосовуються відео та графічні зображення, які оброблялися в спеціальних програмах для висвітлення подій у вигідному світлі [59, с. 123].

Слід зазначити, що в сучасному світі, де технології розвиваються з запаморочливою швидкістю, «фальшива глибока» становить особливу загрозу для громадськості. Цей тип помилкової інформації створюється за допомогою штучного інтелекту і може бути представлений у вигляді зображень чи відео. Основними загрозами, що зважують на поширення глибокої помилки: вони можуть бути створені будь - якою людиною з основними знаннями комп’ютера; простота розповсюдження цієї інформації; І вони настільки правдоподібні, що важко відрізнити їх від справжньої фотографії чи відео. Зрештою, помилкову

інформацію можна легко створити та розповсюджувати через соціальні медіа, що призводить до значного впливу в реальному світі. Згідно з дослідженням Socialbakers, компанія - аналіз, що спеціалізується на детальній статистиці для Facebook, Twitter та YouTube, фальшивих новин поширюється з чотирьох конкретних причин, таких як прибуток, політика, пропаганда та пристрасть. Вони порівнювали найефективніші помилкові та реальні новини, які були опубліковані у соціальній мережі Facebook. Дослідження показало, що 87 % фальшивих новин складали посилання, 10 % фотографій та 3 % відео.

Отже, посилання були типом домінуючих повідомлень, оскільки їхні творці вмісту хотіли залучити користувачів на своєму веб - сайті для отримання доходу. Реальні джерела інформації, як правило, не сприяють їх вмісту в Інтернеті, оскільки вони генерують велику кількість взаємодій органічно [59, с. 126]. Інтернет - платформи вжили багатьох заходів для боротьби з фальшивими новинами та дезінформацією. Зокрема, Facebook, Twitter, Google та Microsoft створили групи фахівців для боротьби з дезінформацією. Незважаючи на зазначені вище факти, під час цих виборів було проведено велика кількість кампанії дезінформації та розповсюдження помилкових новин в Інтернеті.

На початку 2020 року з’явилася нова загроза, яка призвела до розповсюдження помилкової інформації та помилкової інформації - пандемії Ковід -19. Саме в контексті цієї пандемії світ стикався з багатьма складними дилеми, пов’язаними з розповсюдженням пропаганди та дезінформації.

Інфодемія – є надмірною кількістю інформації, включаючи помилкову або оманливу інформацію в цифрових та фізичних середовищах, які поширилися під час епідемії [61, 145]. Це явище стало засобом, що сприяло експлуатації слабких місць цифрових мереж та запуску кібер -атак проти вразливих громад та критичної інфраструктури. Починаючи з лютого 2020 року, інформація про новий вірус та його можливі методи лікування активно поширюється, особливо в соціальних мережах, що спричинило паніку серед населення. За відсутності надійної інформації про походження та поширення коронавірусу в той час соціальні медіа поширювали різну помилкову

інформацію не лише про теорії змови та «нульовий пацієнт», а й на «ефективні» народні засоби проти захворювання.

Отже, важливими загрозами, які є наслідком розповсюдження дезінформації на даний час є:

- швидка розповсюдженість інформації, особливо в соціальних мережах; велика кількість та різноманітність форм дезінформації;
- втручання у політичні події, а саме місцеві, національні, або загальноєвропейські вибори; латентність та підступність стратегій дезінформації.

Ми можемо узагальнити, що боротьба з дезінформацією та помилковими новинами в Україні є актуальною і займає провідне місце, оскільки швидка реакція на ці загрози уповільнює процес поширення помилкової інформації. З іншого боку, боротьба з дезінформацією створює такі проблеми: масштабна дезінформація, тобто, що інформація такого типу поширюється швидкими темпами та всіма можливими засобами спілкування, щоб знати ЗМІ та соціальні мережі; Виявлення та невідповідна відповідь на загрози дезінформації, оскільки, незважаючи на багато затверджених документів та усталених організацій, дезінформація в даний час переважає, оскільки це може бути розповсюджено за допомогою людей.

Це призводить до чергової проблеми, яка виникає в боротьбі з дезінформацією: низький рівень медіа - освіти та критичне громадське мислення. Саме здатність аналізувати та фільтрувати інформацію, що зменшує вплив дезінформації на людей. Отже, одним з головних пріоритетів численних документів, які прийняті, і установи, створені для боротьби з дезінформацією в Україні, - це покращення освіти населення населення. Слід зазначити, що цілеспрямовані зусилля щодо розповсюдження дезінформації та пропаганди включають загрози в кіберпросторі, таких як атаки, онлайн - пропаганда, яка має на меті знищити демократичні системи та чинити руйнівний вплив на суспільство.

Зазвичай, розповсюдження оманливої інформації відбувається в контексті серйозних політичних, соціально-економічних та військових подій. В даний час це все ще викликається війною в Україні. У часи кризи охорони здоров'я дезінформація стає особливо небезпечною. У цей важкий період для всього світу надзвичайно важливо передавати правдиву інформацію громадськості з точністю та вчасно, зокрема, державною владою, оскільки неоплачена комунікація в галузі здоров'я може спричинити негативні наслідки.

Ресурсами для поширення інформації можуть бути традиційні медіа, а також різні онлайн - платформи. Тому важливо виявити, протистояти та запобігти поширенню помилкової інформації в часі. Проте дезінформація являє загрози, які повинні бути бойовими та майстерними в усьому світі, щоб повністю досягти потенціалу технологічного прогресу, поважаючи вираження думок та свободу отримання та розповсюдження інформації. Для початку доцільно ставити під сумнів юридичне та інституційне встановлення механізмів боротьби з дезінформацією та пропагандою.

3.3. Фактчекінг як інструмент протидії маніпулятивним впливам: поняття, концепція, різновиди

Соціальні медіа захопили світ останні п'ятнадцять років. Миттєвий розподіл підроблених новин та оманливої інформації за цими каналами, на жаль, є ознакою нашого часу. Це явище є ризиком демократії, національної безпеки та соціальної тканини, підриваючи довіру громадськості в інформації.

У зв'язку зі збільшенням ролі соціальних мереж, на початку XXI століття у інформаційному просторі виникає концепція пост правди. Дезінформація в Інтернеті - це проблема, яка виходить за межі кордонів, як національної, так і дисциплінарної. Все більш очевидно, що рішення проблеми неможливо знайти без значного міжнародного та міждисциплінарного співробітництва. Таким чином, в контексті інформації та маніпуляційних воєн зростає потреба перевірити точність інформації та фактів, що поширюються в нашому

інформаційному середовищі. Ось чому в 2003 році з'явилася концепція перевірки фактів, що означає перевірку фактів.

Отже, фактчекінг – Це перевірка фактів, щоб забезпечити точний та неупереджений аналіз публічних тверджень для виправлення неправильних публічних ідей та підвищення обізнаності щодо важливих питань. Слід зазначити, що перевірка інформації проводиться на основі офіційних документів [61, с. 150].

У галузі перевірки фактів та перевірки інформації основні стандарти встановлюються Міжнародною мережею перевірки фактів, яка була заснована в 2015 році. Сьогодні вона об'єднує ще сто організацій з 50 країн. Однією з головних умов для учасників є те, що їх редакція не повинна бути під контролем та впливу держави чи політики [61, с. 151].

До основних принципів відносяться:

- Неупередженість та доброчесність (Організації перевірки фактів повинні використовувати той самий стандарт перевірки фактів).
- Прозорість джерел (усі висновки, надані фактами, що підтверджують, повинні бути доступними для читачів).
- Прозорість інформації про джерела фінансування та гарантує, що спонсори не впливають на інформацію в різних дослідженнях організації.
- Чесність у редакційній діяльності.
- Прозорість методології перевірки факту (пояснення методів, що використовуються в процесі перевірки інформації) [61, с. 152].

Перевірка фактів є необхідним механізмом боротьби з дезінформацією. Перевірка фактів має чітку структуру, яка включає: об'єкт дослідження - статтю або публічну декларацію, яку слід перевірити; Основна суть питання - вступна частина, що містить додаткову пояснювальну інформацію; Аргументи, тобто статистика, факти, документи, отримані з офіційних джерел; Висновок - Істина, значною мірою правдива чи хибна, значною мірою хибна чи неможлива перевірка) [56, с. 58]. У цілому, фактчекінгова діяльність в Україні знаходиться лише на стадії розвитку, про це свідчать новостворені організації, різноманітні

проекти, які зосереджуються на аналізі та перевірці інформації. Діяльність обсерваторії базується на таких основних напрямах:

- створення карти фактчекінгових організацій в Україні;

- співпрацювати з обсерваторами для обліку тенденцій в Інтернеті;

- надати рекомендації політичним рішенням - на національному та європейському рівні щодо того, як потенційно покращити свою політичну реакцію на дезінформацію;

- підтримка та координація дослідницької діяльності щодо боротьби з дезінформацією на європейському рівні, включаючи створення та постійне оновлення глобального репертуару дослідницьких статей, а також встановлення звітів про основні результати досліджень; Допоможіть державним органам контролювати діяльність, здійснену онлайн - платформами, щоб обмежити розповсюдження та вплив дезінформації.

Діяльність обсерваторії включає перевірку фактів та медіа -освіту. Обсерваторія створює безпечну онлайн - платформу для виявлення та аналізу кампанії дезінформації. У обсерваторії також є портал, який надає громадянам інформацію та документи, що стосуються підвищення стійкості до дезінформації в Інтернеті та організації заходів для покращення медіа -освіти. [61, с. 775].

Консорціум сприятиме тіснішій співпраці між дослідниками та факт - чеками загалом та в досягнені цілей:

- Створіть кампанії з питань освіти та поінформованості для більш ефективних ЗМІ, враховуючи цифрове та соціальне середовище у кожній державі - членах та в регіоні в цілому.

- Забезпечте загальну методологію дослідникам, які можуть покращити використання баз даних для перевірки фактів в академічному середовищі, а також транснаціональних зусиль для виявлення та демістифікації дезінформації, таких як фальшиві новини та пропаганда.

- Надайте політичні рекомендації, які можуть дати законодавцям кращу основу для їх зусиль для боротьби з розповсюдженням дезінформації.

Отже, Консорціум дозволить академічний аналіз помилкової та оманливої інформації та підтримувати освіту медіа в північних країнах. Таким чином, вищезазначені установи та проекти перевіряють та оцінюють точність інформації на основі фактів та доказів, тим самим випускаючи інформаційний простір для чуток, маніпуляцій, помилкової та оманливої інформації в Інтернеті. Крім того, діяльність з перевірки фактів в Україні не обмежується прийняттям різних документів та створенням проектів чи інститутів, але соціальні медіа також відіграють важливу роль.

Сьогодні соціальні мережі мають значний вплив на поведінку людини. На їхніх просторах ви можете висловити свої думки, свої почуття, публікувати фотографії та відео на різні теми. Крім того, громадськість активно бере участь у створенні та розповсюдженні інформації через соціальні мережі. Отже, за цих умов кількість підроблених новин, помилкова та оманлива інформація в мережі збільшується.

Тому важливо - соціальні мережі сприяють перевірці інформації на своїх платформах, оскільки помилкова інформація може суттєво вплинути на прогрес політичних подій, виборів та психіки людей загалом. Оскільки у Facebook з 2016 року з 2016 року транслюється велика кількість дезінформації та підроблених новин. Facebook, а також Instagram розпочали інтенсивну боротьбу проти поширення дезінформації на своїх платформах та розпочали свої перші факти ініціативи перевірки. Основна мета програми перевірки факту - виявити та усунути вірусну дезінформацію, перевірити точність інформації, що міститься в повідомленнях, щоб люди бачили менше дезінформації в мережах, класифікуючи вміст як «помилковий», «модифікований» або « Частково помилково «так, що в потоках або статтях мереж було менш помітним, вживати відповідних заходів проти повторних дифузорів помилкової інформації, закривши свої рахунки або накладаючи обмеження на сторінки. Facebook

співпрацює з незалежними організаціями перевірки фактів у більшості країн світу [55, с.86].

У той час, як світ охопила пандемія, з 2020 р. у Facebook додали попереджувальне маркування на інформацію, що стосується Covid-19, а також для більш швидкого виявлення порушень стандартів спільноти використовується технологія штучного інтелекту. Крім того, ця соціальна мережа оновила свою політику щодо розповсюдження неправдивої інформації, яка може заважати людям проголосувати на виборах або призвести до насильства, цей тип інформації буде видалений [55, с. 87]. Однак у жовтні 2021 року Марк Цукерберг перейменував у Facebook і змінив ім'я в Meta. Відтепер концепція компанії змінилася, щоб створити мета-вміст, щоб допомогти людям об'єднатися, розвивати бізнес тощо.

Інша платформа, сприятлива для дезінформації та помилкової, - це Twitter, оскільки ця соціальна мережа дозволяє мати кілька облікових записів та бути анонімним користувачем. Google також допомагає боротися з помилковою онлайн - інформацією, повідомляючи статті, що містять помилкову або оманливу інформацію. Незважаючи на заходи, які були вжиті для розробки діяльності для перевірки фактів в Україні, основні проблеми в цій галузі такі:

- повільний процес;
- перевірка фактів може спровокувати зворотний ефект , тобто визначення новини як хибних - приверне увагу та буде розголошена;

На маю думку, треба звернути увагу громадян до нагальної проблеми перевірки інформації та розвитку критичного розуму. Зрештою, критичне мислення допомагає нам розпізнати справжнє та помилкове.

Висновки до розділу 3

Таким чином, аналізуючи дезінформацію як загрозу національній безпеці України, можна зробити наступні висновки, а саме: основним

механізмом протистояння дезінформації та фейковим новинам є всілякі фактчекінгові проекти, компанії у новинних медіа, що мають мету виявити, провірити та спростувати хибну та брехливу інформацію.

Фактчекінг – це перевірка фактів задля забезпечення точного, неупередженого аналізу заяв, щоб виправдати суспільне хибне сприйняття і збільшити знання про важливі питання.

Проаналізувавши головні концепції фактчекінгу можна підвести підсумки, що констатація фактів є найдієвішим засобом протифейкових новин, брехливих даних, помилок і маніпуляцій. Розвиток нових засобів масової інформації можливий лише за допомогою незалежних професійних експертів галузі, які намагаються зробити аналіз якості та відрізнити правду від брехні та маніпуляцій у цьому контексті. Робота незалежних організацій для контролю фактів або окремих дослідників є важливою та відповідною для України. З появою соціальних медіа, дезінформація та помилкові новини поширюються легко та швидко. В даний час соціальні мережі є ефективним джерелом дезінформації. Однак вони постійно розвиваються і намагаються зменшити вплив неправдивої інформації на громадську думку завдяки новим інструментам для перевірки фактів та співпраці з провідними організаціями для перевірки фактів та проекту, що фінансується Україною.

Отже, ефективна боротьба з помилковою інформацією в Інтернеті, соціальних мережах та традиційних аудіовізуальних ЗМІ має велике політичне значення як в Україні, так і в глобальному контексті.

ВИСНОВКИ

Отже, досліджуючи дезінформацію як інструмент гібридної війни можна зробити наступні висновки:

1. У процесі осмислення причин і наслідків інформаційних війн необхідно особливу увагу звернути на зміну ціннісно-смислової матриці життєустрою планетарної спільноти, виникнення явища мережевих відносин. Зазначене зумовлює формування латентного гібридного світу й відповідних форм протистояння у вигляді гібридних конфліктів і навіть гібридних воєн. Зміни у характері планетарної системи обумовлюють глобалізацію свідомості пересічної особистості у напрямі цілісного бачення соціального світу, вироблення Зрілість колективної свідомості, спроможної віддзеркалювати глобалізацію планетарного життя, можливості подолання хибної соціальної та індивідуально зумовленої домінанти. Жоден із інструментів гібридної війни не може розглядатися як чіткий приклад примусового втручання, якщо вона вважається ізольованою справою. Тому важливо, щоб примусовий тиск був виявлений на ранній стадії, проаналізованих і, якщо необхідно, міжнародних та неурядовими державами та установами, що займаються захистом політичної незалежності, гарантованою статутом Організації Об'єднаних Націй швидко і швидко та узгоджено. Крім того, примусовий тиск прозорих та законних дій слід відрізнити від станів, які використовують дипломатичний тиск, що не підпадає під категорію незаконного втручання. Збройний конфлікт в Україні підтвердив тезу про очевидну зміну парадигми в сучасній війні. Навіть якщо активні бойові дії припиняться, Росія буде продовжувати використовувати гібридні методи та методи війни проти України, доки вона матиме політичні та економічні ресурси для цього. Пропагандистський дискурс став новим кроком у розвитку російської енергетичної системи, де паралельно з традиційними

формами пропаганди та агітації використовувались новітні інформаційні технології. Нові конотації та підходи до підвищення ефективності впливу з'явилися в дискурсі: «Документальність», емоція та домінування аудіовізуальної інформації. Як показали події протистояння України та Росією, контроль над її інформаційним простором став не менш (і, можливо, ще більш важливим) у присутності сучасної зброї та навчених військ.

2. Гібридна агресія Росії було пов'язано з бажанням останнього залучити Україну до своїх світових цивілізаційних проектів. Однак українська компанія домагалася іншого геополітичного вектора для розвитку своєї держави, що призвело до соціо - політичного протистояння Майдана. Його перемога змусила Російську федерацію перейти до військового нападу. Це призвело до прийняття Криму та масових заворушень у донецькому регіоні, натхненні пропутіновими силами, що призвело до військового втручання. Автори визначили на сьогодні п'ять етапів збройного конфлікту. Кожен з них має свою логіку через те, що технологія гібридної агресії в донецькому регіоні розвивалася і є динамічною. Його мета - взяти політичний контроль з України. Отже, ситуація постійно змінювалася - масові заворушення з вторгненням «кримської компанії» перетворилися на великі бойові дії, що змусило українську частину розпочати зустрічну. Це призвело до традиційного військового вторгнення в регулярні одиниці російської армії.

Досягнувши цієї мети, Кремль продовжував підніматися на конфлікт, щоб нав'язувати Українській партії умов умови врегулювання ситуації в донецькому регіоні.

Таким чином було підписано «Мінськ-2» статті якого більше відповідали кремлівським інтересам, ніж українським. На останньому етапі офіційна Москва прагне зберегти Україну на своїй геополітичній орбіті через лялькову «Республіку», змінюючи політичну, ідеологічну та соціально - культурну сприйняття окупованої території. Підводячи підсумок, слід зазначити, що аналіз дав можливість зробити наступні висновки щодо формування

юридичних механізмів протидії дезінформації в соціальних медіа в контексті потенціалу Центру боротьби з дезінформацією. Боротьба з дезінформаційними кампаніями з міркувань національної безпеки вимагає поєднання зусиль з боку зазначеного центру, як із предметами національної системи кібербезпеки, так і з органами регуляторних органів ЗМІ, стратегічними комунікаційними підрозділами України у тісній співпраці з Приватний сектор, зокрема, ЗМІ та громадянське суспільство. Навчання юридичних механізмів протидії дезінформації в соціальних медіа в контексті національної безпеки повинно ґрунтуватися на конституційних принципах свободи думки та вираження поглядів з ексклюзивним переліком їх можливих обмежень у соціальних мережах для забезпечення національної безпеки.

3. Основний механізм боротьби з дезінформацією та підробленими новинами складається з різних проектів, організацій та підрозділів для перевірки фактів у інформаційних ЗМІ, які мають на меті визначити, перевірити та спростувати помилкову та оманливу інформацію.

Перевірка фактів полягає у перевірці фактів, щоб гарантувати точний та неупереджений аналіз публічних декларацій, щоб виправити помилкові сприйняття громадськості та дати їй усвідомлення важливих питань.

Проаналізувавши основні поняття перевірки фактів, ми можемо узагальнити, що перевірка фактів є одним із найефективніших інструментів проти фальшивих новин, незвичних даних, введення введення несправностей та маніпуляцій. Зрештою, розвиток нових засобів масової інформації можливий лише за допомогою незалежних професійних експертів у секторі, які прагнуть провести аналіз високої якості і, в цьому контексті, відрізнити істину від брехні та маніпуляцій. Робота незалежних організацій перевірки окремих фактів чи дослідників є важливою та відповідною для України. Тому що з появою соціальних медіа розповсюдження дезінформації та підроблених новин стало легким та швидким. В даний час соціальні мережі є ефективними джерелами дезінформації. Однак вони постійно розвиваються та намагаються зменшити вплив неправдивої інформації на громадську думку, завдяки новим

інструментам для перевірки фактів та співпраці з основними організаціями для перевірки фактів та фінансування проектів через Україну.

Методи гібридної війни не змінюють суть війни. Насильство залишається основою гібридної війни, як і в будь - якій іншій формі війни, і їх мета така ж, як і в будь - якому іншому акті війни, а саме для використання загрози використання, тобто шантаж або використання насильства, організованого отримати фізичні чи психологічні переваги ворога. Однак саме існування термінології - гібридної, асиметричної, нетрадиційної, нелінійної, нового покоління, четвертого та п'ятого покоління, Сіра війна - показує труднощі, які стратеги та теоретики продовжують зустрічатися, щоб класифікувати складні збройні конфлікти 21 століття. Хоча термін «гібрид» в даний час є найпопулярнішим, він на сьогоднішній день не єдиний, хто описує цей тип війни. Той факт, що багато озброєних конфліктів розмивають кордон між війною та миром та інструментами, які традиційно не є частиною війни, ще більше ускладнює це питання. Це, безсумнівно, є викликом для традиційного встановлення сектору безпеки, який повинен зіткнутися з широким спектром загроз, визначених аналітиками та теоретиками Гібридної війни. Якщо мережа визначення занадто широка, термін гібридна війна стає занадто охопленою, щоб використовуватись політичними рішеннями. Якщо визначення занадто близьке, розробники рішень не зможуть зрозуміти важливість багатьох нетрадиційних технологій, що використовуються суперником як доповнення до застосування військової сили.

Незалежно від етикетки, що надається загрозі, стратеги повинні вирішити найкращим чином вирішувати методи, якими користуються суперник, будь то державний чи недержавний актор. Іноді найбільш підходяща відповідь може включати використання політичних, інформаційних, економічних, дипломатичних засобів або, у випадку фізичної загрози, специфічної для держави. Більш складні загрози потребують підходу інтегрованого. Взагалі, найкраща стратегія полягає у координації та керуванні всіма ефективними

інструментами влади та зусиль держави, незалежно від того, як визначається загроза.

Отже, Інформація та культурна безпека нашої країни повинні базуватися на координованій діяльності державних установ та структур громадянського суспільства. Він забезпечує захист національних цінностей та культурних пріоритетів для розвитку національної галузі інформації та культури. Слід зазначити, що в контексті «гібридної війни» роль інформаційної культури як фактор гарантування державного суверенітету значно зростає. Підвищення рівня інформаційної культури українського суспільства об'єктивно сприятиме зміцненню «імунітету» наших громадян проти зброї інформації. Розвиток інформації та культурної безпеки України вимагає, щоб держава приділяла більшу увагу на національну освіту, кіно, мистецтво, літературу та інші підсистеми гуманітарної сфери.

Впровадження нових технологій інформаційної війни не впливає на його традиційні компоненти та цілі. Як і в попередні століття, головне завдання - отримати значні переваги для забезпечення військових, економічних та політичних конфліктів. Незмінність цих постулатів була продемонстрована останніми міжнародними конфліктами, ініційованими Російською Федерацією.

Інформаційна війна проти України ведеться гібридним способом. Гібридна війна - це тип ворожих дій, в якій зловмисник не використовує класичне військове вторгнення, але видаляє опонента, використовуючи комбінацію таємних, саботажних, кібергірських операцій, а також підтримки повстанців, що діють на території противника.

Основні інструменти гібридної війни включають такі інформаційні заходи: засоби військової та політичної дезорієнтації противника; дезінформація про власні ресурси; Дії, спрямовані на запобігання або блокування каналів передачі даних для дезорієнтації та дезорганізації, створення атмосфери напруженості в українському суспільстві від постійних очікувань нападів та масового наступу по всій лінії фронту та впливу на масову свідомість українців до деморалізації та поширення паніка.

Обсяг інструментів гібридної війни: населення конфлікту, заднього населення, міжнародне співтовариство.

Агресор використовував десятки гібридної інформаційної тактики, серед яких слід підкреслити анти - українську та анти - західну пропаганду на масштабні, засновані на доктрині «російського світу». Російські служби військової розвідки створили понад 30 груп та псевдо - українські рахунки в соціальних мережах. Розроблена система антик - української пропаганди та дезінформації мала на меті сформувати образ противника, розділити українське громадянське суспільство, змінити вказівки щодо соціального та політичного розвитку тощо. Ціла серія пропагандистських знімків та знімків стала значними ознаками цієї пропаганди та цієї дезінформації. В рамках інформаційної війни агресор використовує пропаганду війни з боку ЗМІ, а також представниками керівництва країни та політиками та вченими, які близькі йому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Арзуманян Р.В. Определение войны в 21 веке. Обзор XXI ежегодной конференции по стратегии Института стратегических исследований Армейского военного колледжа, 6-8 апреля 2010 / Р.В. Арзумян. – Ереван, 2011. – 60 с.

2. Бедрицкий А.В. Эволюция американской концепции информационной войны // Аналитические обзоры РИСИ. – 2003. – № 3. – 26 с.

3. Боднар Н.А. Проблема ратифікації Римського статуту Міжнародного кримінального суду в світлі європейського вибору України Журнал європейського і порівняльного права.2018. No 8.С. 79–86

4. Герасимов В. Ценность науки в предвидении. Военно-промышленный курьер.2013. 27 лют. (No 8).С. 1–6.

5. Горбань Ю.О. Інформаційна війна проти України та засоби її ведення / Ю.О. Горбань // Вісник НАДУ. – 2015. – №1. – С. 136-141

6. Дорошенко А.С. Гібридна війна в інформаційному суспільстві / А.С. Дорошенко // Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». – 2015. – № 2(25). – С.21-28.

7. Дугин А. Г. Основы геополитики. Геополитическое будущее России. Мыслить Пространством / А. Г. Д угин. – М. : Арктогея-центр, 1999. – 928 с.

8. Зеленін В.В. По той бік правди: нейролінгвістичне програмування як зброя інформаційно-пропагандиської війни. Вінниця: Віндрук, 2014. 384 с.

9. Клаузевіц К. О войне. Фоліо, 2020.640 с.

10. Кудрина Л. (2014) Мариупольские депутаты требуют от Верховной Рады незамедлительных действий для достижения гражданского мира. Приазовский рабочий, No 32 (19806). С. 1-3.

11. Ласвель Г. Техника пропаганды в мировой войне: сокр. пер. с англ. в обработке Н. М. Потапова / Г. Ласвель. – Л.: Отдел военной литературы Госиздат, 1929. – 200 с.

12. Магда Є. (2017) Гібридна агресія Росії: уроки для Європи. Київ, Каламар,268 с.

13. Мак-Люен М. Галактика Гутенберга. Становлення людини друкованої книги. Київ: Ніка-Центр, 2001. 464 с.

14. Маклюен Г. М. Внешние расширения человека / Г. М. Маклюен ; пер. с англ. В. Николаева ; закл. ст. М. Вавилова. – М. ; Жуковский : КАНОН – пресс – Ц, Кучково поле, 2003. – 464 с.

15. Нікитенко В.О. Геокультурні цінності в умовах сучасного світового розвитку: соціально-філософський вимір. Гуманітарний вісник Запорізької державної інженерної академії. 2013. Вип. 54. С. 266–280.

16. Почепцов Г. Г. Психологические войны / Г. Г. Почепцов – М., К.: Рефл-бук, Ваклер, 2000. – 528 с.

17. Пунда Ю. В., Телелим В. М. Основи стратегії національної безпеки і оборони : підручник. Київ : НУОУ, 2016. 596 с.

18. Расторгуев С. П. Информационная война. М., 1998

19. Серажим К. Дискурс як соціолінгвальне явище: методологія, архітектоніка, варіативність. / К. Серажим ; Київ. нац. ун-т ім. Т. Шевченка. – К. , 2002.

20. Смола Л.Є. Аспекти ведення інформаційної та гібридної війни в контексті застосування комунікаційних технологій / Л.Є. Смола // S.P.A.C.E. – 2016. – № 1. – С. 48-53.

21. Ткач В.Ф. Спецпропаганда як інформаційний складник гібридної війни Росії проти України / В.Ф. Ткач // Стратегічні пріоритети. Серія «Політика». – 2016. – №1(38). – 99-109.

22. Ухтомский А.А. Доминанта. Київ; Україна: Наука, 1966. 271 с.

Електронні ресурси:

23. Горбулін В.П. Точка біфуркації. (2016)https://zn.ua/ukr/internal/tochka-bifurkaciyi-_.html

24. Даник Ю., Труш О.О., «Особенности обеспечения национальной безопасности в среде передовых технологий», Государственная организация 1 (2010), Доступно з http://nbuv.gov.ua/UJRN/DeBu_2010_1_42.

25. Динис Г.Г. Проблематика ефективності механізму міжнародно-правового регулювання збройних конфліктів (на прикладі міждержавного збройного конфлікту Росії та Грузії)// Геополітика України: історія і сучасність: збірник наукових праць. Вип. 1. – Ужгород: Ліра, 2009. – С. 61-77. – [Електронний ресурс].- Режим доступу: http;//www.uzhnu.edu.ua›uk/infocentre/get/.

26. Динис Георгій. Агресія Російської Федерації проти України та міжнародно- правові зобов'язання ERGA OMNES Росії перед іншими державами та міжнародним співтовариством . № 4/2014.Український часопис міжнародного права. Науково- практични журнал.ISSN 1814- 3385. Спецвипуск: Міжнародна науково-практична конференція. «Інтереси країни: міжнародно-правовий захист». Київ,06 лютого 2015р. – С. 61-77. – [Електронний ресурс].- Режим доступу: http://jusintergentes.com.ua/index.php?option=com_k2&view=item&id=216:

27. Зубарєва М. А. Аналіз інформаційної війни між Росією та Україною в інформаційному суспільстві. Інформаційне суспільство. 2015. Вип. 21. С. 6-11. URL : http://nbuv.gov.ua/UJRN/is_2015_21_3

28. Котляр В.«К вопросу о гибридной войне» и о том, кто же ее ведет на Украине , стор.5– [Електронний ресурс]. - Режим доступу: https://interaffairs.ru/jauthor/material/1350

29. Макаренко Л.П. Еволюція форм та методів ведення інформаційної війни [Електронний ресурс] / Л.П. Макаренко. – Режим доступу: http://oaji.net/articles/2014/797-1402908125.pdf

30. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс] / В. Петрик. – Режим доступу: http://justinian.com.ua/article.php?id=3222

31. Присяжнюк Д.М. Застосування маніпулятивних технологій з боку Росії в ЗМІ України (на прикладі Криму) / Д.М. Присяжнюк [Електронний ресурс]. – Режим доступу : http://vuzlib.com/content/ view/1108/23

32. Радковець Ю. Гібридна війна Росії проти України: уроки та висновки. (2016). Доступно з https://www.ukrinform.ua/rubric-polytics/2107122-gibridnavijna-rosii-proti-ukraini-uroki-ta-visnovki.html.

33. Шемшученк Ю.С. Закон України «Про порядок висвітлення діяльності органів державної влади та місцевого самоврядування в Україні засобами масової інформації» [Текст] // Інформаційне законодавство: збірник законодавчих актів у 6 томах / за ред.. Т.1, Інформаційне законодавствоУкраїни. К.: ТОВ «Юридична думка», 2005. С. 166-176.

34. Шібель В. Миротворчий процес: методологічні аспекти дослідження. Політичний менеджмент. Вип. 6. (2009). Доступно з http://ipiend.gov.ua/wpcontent/uploads/2018/08/shibel_myrotvorchyi.pdf.

35. Яворська Г.М. Гібридна війна як дискурсивний конструкт. (2016). Доступно з http://ippi.org.ua/sites/default/files/yavorskaya.pdf.

36. Amos C. Fox, Andrew J. Rossow. “Аналіз гібридної війни Росії: оцінка військових дій між Росією та Україною”. The Land Warfare Papers, No. 112 march 2017. The Institute of Land Warfare. Association of the United States Army.Arlington. Virginia.

37. Erika Morphy, (Aug. 24, 2006), Google, Brazil Lock Horns Over Social Networking Data. Tech News World. URL: http://www.technewsworld.com/story/privacy/52624.html.

38. Gehr R. Whymoviesmakethebestjournalism. – ColumbiaJournalismReview, 2015, May 27. http://www. cjr.org/analysis/documentary_journalism.php.

39. Hamilton, Rebecca J., Governing the Global Public Square (March 25, 2020). Harvard International Law Journal. 2021, American University, WCL Research Paper No. 2020-17, Available at SSRN. URL: https://ssrn.com/abstract=3426544

40. Herbert v. Lando, 441 U.S. 153, 168 n.16 (1979).

41. Hoffman F. G. Hybrid vs. compound war [Електронний ресурс] / F. G. Hoffman // Armed Forces Journal, Oct. 2009. – Режим доступу: http://armedforcesjournal.com/hybrid-vs-compound-war/

42. Hoffman F. G. Future Threats and Strategic Thinking [Електронний ресурс] / Hoffman F. G. // Infinity Journal, No Fall 2011. – Режим доступу: https://www.infinityjournal.com/article/34/ Future_Threats_and_Strategic_Thinking/

43. Jack M. Balkin. The Future of Free Expression in a Digital Age. 36 Pepp. L. Rev. Iss. 2 (2009). URL: https://digitalcommons.pepperdine.edu/plr/vol36/iss2/9

44. Jennifer Daskal. Whose Law Governs in a Borderless World? URL: https://constitution center.org/digital-privacy/whose-law-governs-in-a-borderless-world#footnote-24

45. Marvin Ammori. The “New” New York Times: Free Speech Lawyering in the Age of Google and Twitter, 127 HARV. L. REV. 2259 (2014).

46. Max Seddon. Documents Show How Russia’s Troll Army Hit America [Electronicresourse] // BuzzFeed. June 2, 2014. URL : http://www.buzzfeed. com/maxseddon/documents-show-how-russias-troll-armyhit-america

47. Orenstein Mitchell A. The Lands in Between Russia vs. the West and the New Politics of Hybrid War. Oxford UnivercityPress,2019.248 p.

48. Thomas P. Rona. Weapon Systems and Information War / Thomas P. Ro – Boeing Aerospace Co., Seattle, WA, 1976. – 72 p.

49. Wittes B. What is Hybrid Conflict? [Електронний ресурс] // Lawfare. – 11 September 2015. – [Електронний ресурс]. - Режим доступу: https://lawfareblog.com/what-hybrid-conflict