МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ МІЖНАРОДНИХ ВІДНОСИН
КАФЕДРА МІЖНАРОДНИХ ВІДНОСИН, ІНФОРМАЦІЇ ТА
РЕГІОНАЛЬНИХ СТУДІЙ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____ Ніна РЖЕВСЬКА
«____»_____ 2022 р.

КВАЛІФІКАЦІЙНА РОБОТА
ЗДОБУВАЧКИ ВИЩОЇ ОСВІТИ ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА
СПЕЦІАЛЬНОСТІ 291 «МІЖНАРОДНІ ВІДНОСИНИ,
СУСПІЛЬНІ КОМУНІКАЦІЇ ТА РЕГІОНАЛЬНІ СТУДІЇ»
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
«МІЖНАРОДНА ІНФОРМАЦІЯ»

Тема: «ОСОБЛИВОСТІ СУЧАСНИХ ІНФОРМАЦІЙНИХ ВОЄН НА ПРИКЛАДІ УКРАЇНИ ТА РОСІЇ»

Виконавець: здобувачка вищої освіти 4 курсу, 409 Б групи, Ярошович Яна Михайлівна
Керівник: старший викладач кафедри міжнародних відносин, інформації та регіональних студій Ємець Валентина Олександрівна

Нормоконтролер _____ Валентина ЄМЕЦЬ
(підпис)

КИЇВ 2022

ЗМІСТ

ВСТУП

Актуальність теми. На сьогоднішній день інформація відіграє велику роль у житті кожного з нас, вона стала життєво-необхідною для багатьох людей. У XXI ст. інформація стала регулятором усіх соціальних, політичних, економічних та соціальних відносин. Процес розповсюдження інформації на цьому етапі розвивається настільки швидко, що призводить до створення єдиного інформаційного простору. Це, безумовно, позитивно для людства, оскільки швидкий обмін певною інформацією дає можливість людству швидше розвиватись. Однак створення інформаційного суспільства може призвести до багатьох інформаційних катастроф, руйнування духовності суспільства та глобальних технічних катастроф.

Якраз негативні прояви інформаційного простору зароджують таке поняття, як «інформаційна війна», яке на сьогоднішній день стало реальною загрозою безпеці громадянина. Дивлячись за розвитком і наслідками війн і конфліктів у XX і XXI столітті, можна побачити, що роль інформаційного забезпечення стрімко виростає і показує вищий рівень інформаційного конфлікту. Інформаційна війна включає багато факторів, головним з яких є вплив на свідомість людини різними нейролінгвістичними засобами, які мають на меті підірвати цілі та світогляд населення.

Отже, інформаційна війна нині є всеосяжною, цілісною стратегією, яка демонструє важливість володіння інформацією в управлінні, командуванні та реалізації державної політики. Інформаційний конфлікт перетворюється на війну обізнаності, для тих людей, хто буде знати відповіді на найважливіші питання, які дозволяють верхівкам домінувати. Зрозуміло, у такій війні кількість фізичних жертв зводиться до мінімуму, в ній беруть участь всі верстви населення, що може призвести до руйнування суспільства як такого.

Розумна діяльність загального організму населення цілком визначається рівнем розвитку, якістю, захищеністю інформаційного простору, будь-який витік інформації, поширення будь-якої важливої засекреченої інформації серйозно загрожує не лише інформації, а й національній безпеці.

Також, для відстоювання національних інтересів досить широко використовуються інформаційно-психологічні прийоми, а така особливість інформації як масовість призвела до використання у військовій справі інформаційних та комунікаційних технологій. Традиційні види зброї доповнилися новим елементом — інформаційною зброєю. Саме тому дослідження особливостей інформаційних війн, вивчення їх форм та методів сприятиме виробленню методичних рекомендації щодо протидії інформаційного впливу на масову аудиторію та боротьбі з «фейками» в процесі ведення інформаційних війн.

Метою кваліфікаційної роботи є вивчення особливостей сучасних інформаційних війн, а також вироблення методичних рекомендації протидії інформаційним війнам на прикладі інформаційної війни Росії та України

Для досягнення поставленої мети необхідно виконати такі **завдання:**

- визначити методологічну основу та охарактеризувати моделі сучасної інформаційної війни;
- визначити основні положення українського законодавства щодо ведення інформаційної війни;
- проаналізувати методи та способи ведення сучасних інформаційних війн;
- дослідити інформаційну війну між Росією та Україною у період з 2014-2022 роки.
- розробити методичні рекомендації щодо протидії інформаційної війні.

Об'єктом дослідження є особливості сучасних інформаційних війн.

Предметом дослідження виступає інформаційна війна Російської Федерації з Україною

Методи дослідження. Для вирішення окреслених завдань та досягнення мети в роботі були використані такі методи періодизації та класифікації, порівняльний метод, SWOT-аналіз, контент-аналіз.

Структура роботи обумовлена обраною темою, і складається зі вступу, трьох розділів, висновку та списку використаних джерел.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНИХ ВІЙН

1.1 Методологічна основа сучасної інформаційної війни

На сьогоднішній день інформація набуває матеріальної форми, і володіння інформацією стає дуже бажаним. Будь-які, цілком «відчутні» рішення сьогодні будуть апробовані в інформаційному полі. І результати мають вирішальне значення. Інформаційно-комп'ютерна революція відкриває широкі можливості для впливу на людей і владу, маніпулювання свідомістю та поведінкою людей навіть у віддалених районах країни. Враховуючи глобалізацію телекомунікаційних мереж у світі, можна припустити, що інформаційна агресія буде пріоритетом у майбутньому і головною зброєю проти влади. Це питання вимагає серйозної уваги з боку різних експертів, щоб уникнути найбільш негативних наслідків цієї війни для всього людства.

Сьогодні для функціонування міжнародних відносин інформація є об'єктом і суб'єктом водночас, а це важливим механізмом регулювання зовнішньої політики держави. А самі ЗМІ є новими «природними ресурсами», які збільшують багатство суспільства.

У той же час, інформаційна війна, має тисячолітню історію. Приклади інформаційного впливу на морально-духовну стійкість ворога можна знайти як у Стародавньому Римі, так і в епоху феодалізму (боротьба з «єрессю», за «істинну віру» тощо), так і в пізніші часи. Інформаційні війни набули особливого значення в XX столітті, коли газети, радіо, а згодом і телебачення ставали ще більш впливовими.

Інформаційні війни супроводжували всю історію людства. Спочатку вони були релігійно-ідеологічними, використовували всілякі репресії для боротьби з іноземними поглядами. У далекому минулому інквізиція або репресивний апарат тоталітарних держав XX століття вели активну боротьбу з носіями чужорідних ідей.

Як результат, процеси прийняття рішень стали найбільш вразливим місцем у функціонуванні сучасних міжнародних відносин. Сама інформація як така поступово

почала змінювати свій статус: трансформувавшись з фізичної сили, яка допомагає в бою, до розумової головної сили, яка вирішує результат війни.

Інформаційна війна носить пропагандистський характер. Наприклад, перебіг «холодної війни» будувався з використанням пропагандистських механізмах, бо механізми гарячої війни не використовувалися. До речі, потреба в пропаганді в часи «холодної війни» дала значний поштовх до розвитку теорії комунікації, оскільки у сфері комунікації існувала велика кількість суто прикладних завдань.

Термін «інформаційна війна» вперше з'явився наприкінці 1980-х років. Термін активно використовувався під час військової кампанії США в Іраку 1991 року, де вперше були використані не тільки інформаційні технології, а й відкрито підкреслювалося поняття «інформаційна війна», що викликало ще більший резонанс.

Перш за все, коли йдеться про будь-яку війну, в тому числі й інформаційну, треба говорити про певний стан відносин між супротивниками. Інформаційна війна виникає в результаті нових підходів до використання інформації, визначення її ролі та місця. Існує два тлумачення поняття інформаційної війни: гуманітарне та технічне.

Наприклад, М. Ю. Павлютенкова зазначає, що в гуманітарному розумінні інформаційна війна є активним методом перетворення інформаційного простору, що виражається в системі інтрузивних моделей світу, покликаних забезпечити бажану поведінку, атаки на структури генерації інформації. Технічне тлумачення цього поняття полягає в тому, що за допомогою спеціальних програм руйнують апаратні, програмні засоби тощо.[1]

Що стосується іншого розуміння поняття інформаційної війни, тобто технічного, передумова полягає в тому, що інформаційна війна є результатом узгоджених дій щодо використання інформації як зброєю війни в кожній сфері життя. Інформаційна війна включає в себе такі дії:

- вплив на інфраструктуру систем життєзабезпечення – телекомунікації, транспортні мережі, електростанції тощо;
- промислове шпигунство – порушення прав інтелектуальної власності, крадіжка запатентованої інформації, спотворення або знищення важливих даних, проведення конкурентної розвідки;

– хакерство – злом та використання персональних даних, ідентифікаційних номерів, інформації з обмеженим доступом тощо.

Також можна зустріти й інші думки на рахунок поняття інформаційної війни. На думку дослідника А.А Кокошина вперше такий термін як «інформаційна війна» було введено в 1985 році в Китаї. Теоретичні підходи китайських фахівців у сфері інформаційної війни базуються на поглядах стародавнього китайського полководця Сунь Цзи. Він першим узагальнив досвід інформаційного впливу на противника.

На початку 1990 років термін «інформаційна війна» з'явився в США і став головною частиною міжнародної практики. На сьогодні цей термін використовується у двох площинах:

У широкому сенсі – визначити протистояння в інформаційній сфері в ЗМІ для досягнення різних політичних цілей;

У вузькому розумінні – для визначення військового протистояння у військово-інформаційній сфері для досягнення односторонніх переваг у отриманні, зборі, обробці та використанні інформації на полі бою (в операціях, боях).

У вітчизняній практиці в широкому сенсі найчастіше вживається термін «інформаційне протистояння»; у вузькому розумінні – «інформаційні військові дії».

Враховуючи таке визначення можна зазначити, що інформаційне протиборство включає в себе три незмінні складові: 1) вплив; 2) аналіз; 3) протиборство.

Американські науковці визначають, що інформаційна війна це як «нефізична атака на інформацію, інформаційні процеси та інформаційну інфраструктуру», оскільки «метою інформаційної війни є вплив на систему знань та уявлень зовнішнього ворога».[2] Під знаннями тут розуміють об'єктивну інформацію, загальну для всіх, а ідеї - інформацію, яка є суб'єктивною.

Під суб'єктами інформаційної війни можна розуміти суспільство, певні групи суспільства, об'єднані спільними інтересами чи іншими ознаками (національність, мова, професія, територіальне розташування тощо), країни, групи країн, міжнародні організації, які мають суттєві суперечки з іншими або які вступають у фазу

конкуренції, використовуючи всі властивості інформації, інформаційних ресурсів і новітніх інформаційно-телекомунікаційних технологій (інформаційна зброя).[3]

Варто зазначити, що суб’єкти інформаційної війни мають ряд особливостей, які істотно відрізняють їх від інших суб’єктів. Так, зокрема, Бутранець В.К. включає такі характеристики:

- розробка інформаційної зброї, засобів її доставки, замаскування або володіння інформаційною зброєю;
- наявність у суб'єкті спеціальних підгруп або структур, які функціонально уповноважені вести інформаційну війну;
- суб'єкт має власні інтереси в інформаційній сфері та інших сферах життя;
- контроль суб'єктом тієї частини інформаційного простору, в якій він наділений першочерговим правом встановлювати правила регулювання відносин;
- наявність в офіційній ідеології положень, що дозволяють суб’єкту брати пряму чи опосередковану участь в інформаційній війні.[11]

До суб’єктів в інформаційних війнах, науковці відносять:

- держави, їх союзи та коаліції;
- міжнародна організація;
- недержавні незаконні (у тому числі незаконні міжнародні) збройні формування та організації терористичного, екстремістського, радикально-політичного, радикально-релігійного спрямування;
- транснаціональні корпорації;
- віртуальні соціальні спільноти;
- медіа-корпорації;
- віртуальні коаліції [12, с.281]

Держави, їх альянси та коаліції, які є одними з найбільших акторів інформаційних воєн, характеризуються присутністю стійких інтересів в інформаційному просторі. З метою підтримки особистих інтересів в інформаційному середовищі, запобігання їх становлення немалої загрози чи боротьби з недоторканністю цих інтересів країни їхні союзи та коаліції розробляють та здійснюють низку заходів, зокрема:

- формування власного інформаційного простору (державного, союзного чи коаліційного), який об'єднаний у глобальний інформаційний простір;
- контроль за належним функціонуванням інформаційного простору;
- розроблення відповідної нормативно-правової, концептуальної, ідеологічної бази, яка регулює випадки участі в інформаційній війні, визначає основні принципи та форми участі в інформаційній війні суб'єкта;
- створення спеціальних структурних підрозділів (як у складі силових структур, так і у складі державних органів), основною яких є управління інформаційна війна;
- розробка різноманітних інструментів управління інформаційна війна (інформаційна зброя) або, якщо самостійно виготовити інформаційну зброю неможливо, її придбання (легально чи незаконно) для кордону

В цілому об'єкт це те, на що скеровано певну активність, а в цьому випадку – те, на що суб'єкт інформаційної війни намагається подіяти з метою досягнення позитивного результату для самого суб'єкта. Таким чином, ми можемо сказати що головний об'єкт, на якому концентрується безпосередній інформаційний деструктивний вплив у межах заходів інформаційної війни, – громадська думка та свідомість окремої людини.

Дослідники інформаційних воєн поділяють об'єкти інформаційної війни на:

- об'єктами вибухової діяльності є різні типи колективних відносин, правопорядок, безпека, боєготовність, боєздатність збройних сил та інших воєнізованих формувань, органів безпеки та правопорядку тощо;
- об'єктами негативного інформаційного впливу є люди, його соціальні, національно-етнічні, релігійно-конфесійні групи, верстви чи окремі особи, особливо лідери останніх.[11]

Науковці в цій галузі, поділяють об'єкти інформаційної війни на: загальні об'єкти, спеціальні об'єкти, об'єкти розвідувальних спрямувань.

Отже, спільними об'єктами є правопорядок, старанна діяльність влади та адміністрації, мобілізаційна готовність і боєздатність армії, служби безпеки та правоохоронних органів, налагоджені міжнародні зв'язки, світовий престиж.

До особливих об'єктів відносять громаду в цілому та його окремі шари, верстви, групи індивідів, їх окремих представників. Це може бути той чи інший етнічний чи соціальний прошарок або навіть певні групи людей, у тому числі засуджені, безпритульні, сектанти, політизовані радикали від націоналістів, анархісти тощо.

На рахунок об'єктів розвідувального проникнення, то в сакраментальному розумінні такі об'єкти інформаційної війни визначити досить важко. Ними можуть бути установи та організації, які безпосередньо виступають у ролі проміжної ланки між окремою персоною чи населенням взагалі та інформаційними масивами тощо.

Основним інструментом інформаційної війни є інформаційна зброя. До «інформаційної зброї» можна віднести:

- Засоби інформаційно-технічного характеру, які знищують, спотворюють або крадуть інформацію, незалежно від системи захисту, обмежуючи доступ до цієї інформації для легітимних користувачів.
- Безперечно, інформаційно-психологічні засоби, які дезорганізують інформаційні системи шляхом дезінформації, формування хибних логічних інформаційних понять, інтерпретацій тощо, впливаючи таким чином на громадську думку, життя суспільства, держави чи групи держав у цілому.

Таким чином, інформаційна зброя – це пристрої та засоби, які призначені для нанесення максимальної шкоди противнику під час інформаційної боротьби (за допомогою небезпечних інформаційних впливів).[4]

На сьогодні поняття «інформаційна війна» можна обґрунтувати по-різному. Це зумовлено багатозначністю терміну, що породило безліч понять при його перекладах. Зазначене поняття може трактуватися як «інформаційна війна», «інформаційне протиборство», «інформаційно-психологічна війна». Можна сказати, що інформаційна війна характеризується як інформаційна діяльність, що вживається політичною освітою (наприклад державою) для послаблення, руйнування іншого політичного утворення; як інформаційна протидія між учасниками змагання конкурентами; інформаційний військовий конфлікт між двома масовими ворогами, наприклад арміями і т. п. [5.с. 239]

Результати теоретичного аналізу дозволяють стверджувати, що існують дуже аргументовані концепції інформаційної війни і немає загального визначення цього поняття. Таке різноманіття підходів зумовлене насамперед складністю об’єкта дослідження, а також теоретико-методологічними позиціями авторів, що належать до різних наукових шкіл.

Метою інформаційної війни є ослаблення моральних і матеріальних сил противника та зміцнення своїх власних. Передбачаються заходи щодо розвитку свідомості людини в світоглядних та емоційних сферах. Очевидно, що інформаційна війна є невід'ємною частиною ідеологічної боротьби, вона не веде безпосередньо до кровопролиття, руйнувань, проходить без жертв, нікого не позбавляє їжі, даху над головою. Між тим руйнування, викликані інформаційними війнами в соціальній психології, психології особистості, за масштабами і значенням цілком однакові, а іноді і перевищують наслідки збройних воєн.

Головним завданням інформаційних воєн є маніпулювання масами. Метою такої маніпуляції часто є:

- впровадження в суспільну та індивідуальну свідомість ворожих, шкідливих ідей і поглядів;
- дезорієнтація та дезінформація мас;
- ослаблення певних переконань, основ;
- залякування свого народу в образі ворога
- залякування ворога своєю силою. І останнє, але не менш важливе завдання
- забезпечити ринок збуту для вашої економіки.

У цьому випадку інформаційна війна є частиною змагання[6].

Інформаційна кампанія – це серія системних інформаційних інтервенцій (внутрішніх чи зовнішніх, або одночасно тих і тих). Інформаційна кампанія налаштована на зміни в фізичному просторі за допомогою внесення змін в інформаційний та віртуальний простори.

Успішна інформаційна кампанія на основному рівні підтримує стратегічні цілі, впливаючи на здатність противника швидко та якісно приймати рішення. Іншими словами, метою інформаційної війни на оперативному рівні є створення таких

перешкод для процесу прийняття рішень конкурентом, щоб противник не міг діяти чи вести війну швидко та ефективно. В інформаційній війні метою є узгодження дій на оперативному рівні з діями на стратегічному рівні, щоб у своїй сумі вони змушували супротивника приймати рішення, які б призвели до дій, які допомагають суб'єкту досягти його власних цілей і заважають противнику досягти своєї заданої цілі.

Що стосується мети інформаційних війн, то чим більше ворог залежить від інформаційних систем у прийнятті певних рішень, тим він уразливіший до ворожих маніпуляцій цими системами. Програмні віруси впливають лише на системи, у яких є дані програми.

Чим сучасніше суспільство, тим більше воно покладається на інформацію та засоби отримання певних новин. Сюди входить мережа Інтернет, але це лише верхівка айсберга. Кожна розвинена країна має телефонні, банківські та багато інших керованих комп'ютером мереж, тому вони мають свої слабкі сторони.

Загальна мета інформаційної війни в такий спосіб – порушити обмін інформацією на території противника. Неважко зрозуміти, що цей вид зброї зазвичай не спрямований на втрату живої сили. У цьому сенсі технологічна крива нарешті привела до безкровної і водночас надзвичайно ефективної зброї. Знищує не населення, а державний механізм.

Специфічне озброєння використовується в стратегічних інформаційних війнах. Ця зброя не завдає фізичної шкоди, але може призвести до справжньої війни.

Інформаційна зброя – сукупність спеціалізованих (фізичних, інформаційних, програмних, електронних) методів і засобів для тимчасового або безповоротного виведення з експлуатації функцій або служб інформаційної інфраструктури в цілому або окремих її компонентів.[7]

Головною дією інформаційної зброї є відчуження або спотворення інформаційних потоків і процесів прийняття рішень противником.

З настанням нового тисячоліття значення інформації для суспільства активно зростає, саме тому відбувається перехід від звичайної зброї до нової – інформації, зброї штучного інтелекту. Роль інформації в розумінні її впливу на бойові дії стала

настільки значною, що, наприклад, під час операції «Буря в пустелі» іракські втрати становили 35%, а бойовий дух впав аж на 60%. Вона залучила 2500 радіопередач і розповсюдила 30 мільйонів листівок.

Нові інформаційні системи та технології – електронні засоби масової інформації, Інтернет, мобільний зв'язок, глобальна навігація – ще більше розширили можливості інформаційних засобів у війні. Це дозволяє промислово розвинутим державам, таким як США та Японія, значно підвищити свою політичну, економічну та військову перевагу через лідерство в інформаційному просторі, а також встановити глобальний інформаційний контроль над світом і таким чином встановити свої бажані правила в реальному світі. І це тривожить менш розвинені країни, адже їхня ідентичність, незалежність і суверенітет під загрозою тому вони мають активно підвищувати інформаційну безпеку.

Дослідивши генезис поняття, сформулюємо визначення інформаційної війни. Отже, інформаційна війна – це використання та управління інформацією з метою отримання конкурентної переваги над противником.

Інформаційна війна може включати: збір тактичної інформації; забезпечення безпеки власних інформаційних ресурсів; поширення пропаганди чи дезінформації з метою деморалізації армії та населення противника; підриву якості інформації противника та запобігання можливості збору інформації противником.[8]

Дослідивши поняття «інформаційної війни», спробуємо визначити її загальні характеристики:

- психологічний вплив на будь-яку аудиторію (народ, військовослужбовців, робітників, інтелігенцію тощо).
- контроль над інформацією.
- стратегія застосування інформаційних засобів носить лише наступальний характер.
- цілі ведення інформаційної війни – формування світогляду суспільства і використання його в своїх цілях.
- захист власного інформаційного простору від нападу. [6]

Існують й інші класифікації складових інформаційного конфлікту:

- психологічні дії– використання інформації для впливу на аргументацію солдатів противника.
- електронна війна – використання різних засобів, що не дозволяють ворогові отримати точну інформацію.
- дезінформація – надання противнику недостовірної інформації про сили й наміри.
- фізичне знешкодження – може бути частиною інформаційної війни, якщо має на меті вплив на компоненти інформаційних систем.
- заходи безпеки – прагнення уникнути того, щоб ворог дізнався про можливості та наміри.
- прямі інформаційні наступи – пряме перекручування інформації без вагомої зміни сутності, в якій вона знаходиться.

Інформаційна зброя кардинально відрізняється від усіх інших засобів поведінки війни, які з її допомогою можна вести (і вже ведуться) неоголошені і найчастіше невидимі світові війни і цілі цієї зброї є понад усе громадянські інститути суспільства і держави – економічні, політичні, соціальні тощо.

Інформаційно-комп'ютерна революція відкриває широкі можливості для впливу на народ та владу, маніпулювати свідомістю та поведінкою людей, навіть на віддалених просторах. Враховуючи процес глобалізації телекомунікаційних мереж, що відбувається в світі, можна сказати, що саме інформаційним видам агресії буде відданий пріоритет у майбутньому. Потрібна серйозна увага фахівців різних профілів поки що, щоб уникнути негативних наслідків цієї війни для всього людства.[9]

Можна стверджувати, що цілі інформаційної війни значно відрізняються від воєн у загальноприйнятому розумінні. Це не фізичне знищення противника та ліквідація його збройних сил, не знищення важливих стратегічних та економічних об'єктів, а масштабне порушення роботи інформаційних, комунікаційних мереж і систем, часткове порушення економічної інфраструктури та підпорядкування ворогам, населення відповідно до волі країни-переможниці.

Крім того, в епоху інформаційних воєн бойові плани розробляються військовими разом із цивільними спеціалістами, причому останні часто відіграють у цьому провідну роль.[13]

1.2. Українське законодавство в галузі інформаційної безпеки

Інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та технології мають значний вплив на рівень і темпи соціально-економічного, науково-технічного та культурного розвитку. Тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий за умови захисту інформаційної безпеки. Сучасний етап генезису суспільства характеризується неухильним посиленням впливу інформаційної сфери, до якої входять: інформація, інформаційні посилання та інформаційні системи, сайти, що беруть участь у підготовці, зберіганні, поширенні та використанні інформації та інформаційних посилань. Національна безпека держави має сильну залежність від інформаційної безпеки, яка постійно зростає з розвитком інформаційних технологій. Для ефективного забезпечення національної безпеки в інформаційній сфері необхідні відповідні висококваліфіковані фахівці.

Термін «національна безпека» можна використовувати відносно масштабного кола громадських систем для характеристики їхнього захисту від різних негативних факторів природного та соціального характеру. Цей термін характеризує рівень захищеності життєво значущих інтересів, прав і свобод особи, суспільства і держави від зовнішніх і внутрішніх загроз або ступінь відсутності загрози правам і свободам людини, головними інтересам і цінностям населення. Поняття «національна безпека» можна розглядати як своєрідну властивість динамічних систем, комплексних критерій оцінки їх якості та ефективності.[14]

Під терміном національної безпеки ми можемо розуміти, що це можливість громадян задовольнити свої потреби самозбереження, самовідтворення та самовдосконалення з мінімальним ризиком пошкодження основних цінностей свого поточного стану.

Політолог Н. Косолапов говорить, що термін «національна безпека» це — стабільність, яку можна підтримувати в будь-який час протягом тривалого часу, стан цілком розумної динамічної захищеності від найістотнішого з реальних наявних загроз, небезпек та можливості визначати проблеми та вчасно вжити заходів щодо їх нейтралізації.[15]

Закон України «Про національну безпеку України» від 21 червня 2018 року. № 2469-VIII поняття «національна безпека» сформулював набагато коротше без переліку національних інтересів: «національна безпека Україна — захист державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз».

Сьогодні як мінімум три основні теоретичні підходи до розуміння сутності національна безпека.

Перший підхід, представлений А. Вулферсом, Д. Гедді, Г. Деєм, Дж. Джонсоном, Д. Кауфманом, Р. Коеном, М. Міхалком та іншими, вони зосереджується на захисті цінностей суспільства. Серед основних цінностей політична незалежність, економічне процвітання, розвиток, справедливість та інші. При цьому безпека визначається не лише як захист національних цінностей, а й як їх безперешкодне поширення [16].

Інформаційні ресурси України – це вся загальна інформація, яка належить нашій державі, незалежно від змісту, форм, часу та місця створення, поширення та зберігання. Україна самостійно формує та розпоряджається інформаційними ресурсами на своїй території, крім випадків, передбачених законодавством та міжнародними договорами. [17, ст8]

Національні інформаційні ресурси – це загальна інформація про суверенітет України. Одним із найважливіших чинників, що є основою державної політики в інформаційна діяльність, інформаційна інфраструктура.[16] Інформаційна структура є невід'ємною складовою як інструментів стратегічної інформації, що є основою обороноздатності країни, так і інформаційного ринку, який сьогодні значною мірою визначає економічний потенціал та перспективи країни.

Так, Законом України «Про національну програму інформатизації» окреслені основні складові національної інформаційної інфраструктури (національної інфраструктури інформатизації), що включає[18]:

- міжнародні та міжміські телекомунікаційні і комп'ютерні мережі;
- систему інформаційно-аналітичних центрів різного рівня;
- інформаційні ресурси;
- інформаційні технології;
- систему науково-дослідних установ з проблем інформатизації;
- виробництво та обслуговування технічних засобів інформатизації;
- систему підготовки висококваліфікованих фахівців у сфері інформатизації.

Інформаційна безпека – захист інформації в організації або технічній системі від несанкціонованого доступу (перевірка, крадіжка, зміна, знищення). Державним стандартом України прийнято таке визначення терміну «інформаційна безпека» – країна, яка захищає інформацію від загроз їй. Інформаційна безпека забезпечується шляхом захисту інформації від випадкового або навмисного доступу неуповноважених осіб для отримання, розголошення, зміни або знищення важливої інформації. Впровадження вимог та правил щодо захисту інформації, підтримки інформаційних систем у захищеному стані, експлуатації спеціальних технічних та програмно-математичних засобів захисту та забезпечення організаційно-технічних заходів із захисту інформаційних систем, що обробляють інформацію з обмеженим доступом у недержавних структури.[19]

Захист інформації – це комплекс правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний доступ до неї.[17, ст10]

Інформаційна безпека суспільства – це можливість для суспільства та окремих його членів вільно реалізувати свої конституційні права, пов'язані з вільним отриманням, обробкою, створенням і поширенням інформації, а також ступінь їх захищеності від руйнівного інформаційного впливу. Необхідний рівень інформаційної безпеки суспільства забезпечується комплексом політичних, економічних, організаційних заходів, спрямованих на запобігання, виявлення та

нейтралізацію тих обставин, факторів і дій, які можуть завдати шкоди чи зашкодити інформаційним правам, потребам та інтересам країни та її громадян. Варто зазначити, що інформаційна безпека особистості та суспільства тісно пов'язані.[17, ст.11]

Інформаційна безпека суспільства і людей залежить від рівня:

- інтелект, спеціальна теоретична та практична підготовка;
- критичне мислення, моральне та духовне вдосконалення;
- гармонійний розвиток особистості в суспільстві;
- технічні засоби захисту.

Інформаційна безпека держави – це стан її безпеки та інформаційного розвитку, за якого дії інформаційного впливу, спеціальні інформаційні операції, інформаційні війни, інформаційний тероризм, незаконне отримання інформації спеціальними технічними засобами та комп'ютерні злочини не завдають істотної шкоди до національних інтересів. Необхідний рівень інформаційної безпеки забезпечується створенням умов для гармонійного розвитку інформаційної інфраструктури держави, реалізації конституційних прав і свобод людини в інтересах країни: зміцнення конституційного ладу, суверенітету та територіальної цілісності держави, утвердження політичну та соціальну стабільність, економічний розвиток, беззастережна правоохоронна діяльність та міжнародне співробітництво.

Існує два аспекти тлумачення інформаційної безпеки в контексті національної безпеки. З однієї сторони, інформаційна безпека розглядається як самостійний елемент національної безпеки кожної країни, а з іншої – як інтегрований компонент будь-якої іншої безпеки: військової, економічної, політичної та ін. Визначення інформаційної безпеки є оптимальним і відображає всі сторони взаємодії суб'єктів інформаційних відносин. Зосередження на проблемі інформаційної безпеки України зумовлена антиукраїнськими впливами, які сприяють сепаратизму, насильству, національній ворожнечі та є спробами знищення національної ідентичності України, руйнування етнічної злагоди, посягання на конституційний лад України, територіальний цілісний стан України.

Проблема забезпечення інформаційної безпеки України є актуальною у війні, коли Російська Федерація розширила інформаційне та необ'єктивне висвітлення

фактів і явищ, і технологій російських інформаційно-психологічних операцій, спрямованих на домінування над українськими (і світовими) інформаційними просторами та збереження переваг у ЗМІ. Російські пропагандистські інформаційно-психологічні кампанії, акції та медійні заходи впливають не лише на суспільну свідомість громадян України, а й на світову спільноту в цілому.[20]

Аналіз ситуації в інформаційному просторі України свідчить про існуючі проблеми у сфері захисту національної інформаційної безпеки. Особливо це стосується асиметрії інформаційних потоків: мова йде про потужний інформаційний вплив прилеглих країн на внутрішню громаду та відсутність адекватних інформаційних каналів з України до міжнародної діаспори.

Прийом державних українських телерадіопрограм на території Російської Федерації значно менша, ніж російських програм на Сході України, оскільки Україна не має належної технічної бази для трансляції таких програм на території Росії. Присутність «Голосу Росії» та ТРК «Співдружність» в інформаційному просторі РРТ в інформаційному просторі України як за обсягом мовлення, так і за пропускною здатністю мережі в декілька разів вища, ніж у державних телевізійних каналах нашої країни.

Важливим аспектом інформаційної безпеки є безпека інформаційного обміну в спеціальних системних зв'язках та системах загального користуванням. Сьогодні в Україні створюються та експлуатуються спеціальні телекомунікаційні системи в усіх можливих міністерствах і відомствах. Серед них міністерства оборони, внутрішніх справ та надзвичайних ситуацій.

Конституція України (ч. 1 ст. 17) визначає завдання забезпечення інформаційної безпеки як одну з найважливіших функцій країни і діяльності всього українського народу, що обумовлено її основним місцем у системі національної безпеки:

- національні інтереси, загрози їм та захист від цих загроз у всіх сферах реалізуються шляхом своєчасної оперативної інформації та інформаційної сфери в цілому;

- інформація та інформаційні системи та права на них - основні об'єкти безпеки в усіх її формах і проявах;
- завдання національної безпеки вирішуються за допомогою різних класів інформаційних ресурсів та інформаційних підходів як основного науково-практичного методу;
- питання національної безпеки тісно пов'язані з питаннями міжнародної безпеки, які зараз набувають сильного інформаційного характеру.

Невирішеною проблемою залишається забезпечення належного темпу розвитку національних інформаційних засобів та відповідної інфраструктури. В Україні остаточно не вирішено проблему запровадження сучасних інформаційно-аналітичних технологій місцевого управління, що негативно вплинуло на взаємодію гілок влади, формування цілісної вертикалі ефективної виконавчої влади, ефективність політичних та економічних реформ, суспільства та інших сфер суспільного життя.

Україна прагне до продуктивної міжнародної співпраці в інформаційній сфері з урахуванням досвіду найбільш розвинених країн (США, Канади, Японії, Німеччини, Франції, Англії). Йдеться про підтримання динамічної конкуренції, забезпечення відкритого доступу до інформаційно-телекомунікаційних систем та універсального доступу до інформаційних продуктів і послуг.

У нинішній ситуації в Україні через повномасштабну війну Російської Федерації особливо важливо протидіяти поширенню шкідливої для психічного стану людини інформації, що не заборонено вважати перебільшенням інформаційної зброї, а також розробці відповідного законодавства. Україна повністю відчула всю глибину загрози такого постійного, цілеспрямованого, продуманого та фінансованого впливу з боку Російської Федерації під час анексії Криму, військових дій на сході України в 2014 році та повномасштабного вторгнення на територію України 24 лютого 2022 року Саме тому, питання протистояння інформаційним впливами, мають бути передбачені в спеціальному законі про інформаційну безпеку.

Іншою проблемою, яка вимагає законодавчого визначення та врегулювання, є відсутність систематизації законодавства щодо протидії екстремізму в інформаційній сфері. Як наслідок, матеріали такого змісту часто майже безперешкодно

поширюються, оскільки діяльність щодо застереження та припинення різних видів екстремізму здійснюється компетентними державними органами безсистемно, а часто й формально. При цьому важливо пам'ятати, що справжня протидія екстремістським чи іншим негативним проявам в інформаційній сфері не має перетворюватися на зведення особистих рахунків із «незручними» журналістами, тиск на опозиційні ЗМІ та придушення свободи слова.

Процес інформаційного товариства потребує чіткого правового регулювання різноманітних відносин, що виникають у результаті створення, функціонування, використання інформаційних систем і ресурсів, протоків зв'язку, відповідних технологій тощо. Формування такої підгалузі в системі інформаційного права, як правове забезпечення інформаційної безпеки, потребує виокремлення законодавчих, нормативно-правових актів, норм, що регулюють різні фактори інформаційної безпеки, аналізу їх системних недоліків, а також систематизація, консолідація на цій основі загальноприйнятих правових норм в єдиний основний закон, вільний від наявних протиріч, колізій та упущень. Такі дії, у свою чергу, мають забезпечити передумови для якісної загальної трансформації законодавства, що регулює інформаційні відносини в різних сферах суспільства.

Узагальнюючи міркування щодо українського законодавства в галузі інформаційної безпеки, слід зазначити, що прийняття Основного Закону України «Про інформаційну безпеку України» необхідне для закріплення, удосконалення відповідного законодавства, чіткої структуризації законодавства у цій сфері, усунення невідповідностей, упущень та інші недоліки. Цей закон, на мою думку, має закріпити найзагальніші положення, які стосуватимуться інших нормативно-правових актів у цій галузі, а саме: принципи правового забезпечення, структуру відповідного законодавства, загальні параметри безпеки правової інформації, єдину термінологію. Для чіткого поняття даного терміну, та для розуміння громадян що за собою несе інформаційна війна, в законі України повинне бути зрозуміле формулювання інформаційних війн.

РОЗДІЛ 2. ОСОБЛИВОСТІ ВЕДЕННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ВІЙН

2.1 Форми та види сучасних інформаційних війн

Інформаційна війна сама по собі не є абсолютно новим явищем, але її можна простежити в давній історії. Інформаційна частина була присутня в протистоянні давніх племен, релігій і народів. Проте з розвитком технологій мінялись засоби та сам процес ведення інформаційної війни. Коли тисячоліття тому «слово» використовувалося як засіб досягнення даної цілі в інформаційній кампанії, сьогоднішні інструменти інформаційної війни, окрім засобів масової інформації, стали програмно-технічними засобами, які стали визначальним компонентом сучасного інформаційного протистояння.

Інформаційні операції зараз стали важливою частиною військових стратегій багатьох країн. Новітні досягнення науки та техніки привели до революційних змін у всіх сферах нашого життя. Інформаційний розвиток технологій змінив звичні критерії оцінки військової могутності. Змінилися й традиційні форми збройної боротьби. Міжнародні події останнього десятиліття та сучасності показали, що технологічна і, перш за все, інформаційна перевага відіграють вирішальну роль у досягненні цілей воєн і збройних конфліктів.

За умов трансформації інформаційної війни змінюються також її форми. І саме так з розвитком інформаційної війни можна виділити два покоління інформаційної боротьби. Для інформаційного протистояння першого покоління притаманне:

- вогневе придушення (у воєнний час) елементів інфраструктури державного та військового управління;
- ведення радіоелектронного протистояння;
- одержання розвідувальної інформації шляхом перехоплення й декодування інформаційних хвиль;
- здійснення несанкціонованого доступу до інформаційних ресурсів з наступною їх фальсифікацією чи викраденням;

− масове подання в інформаційних каналах противника чи всесвітніх мережах дезінформації для впливу на людей, які приймають важливі рішення;

− одержання інформації від перехоплення відкритих джерел інформації.

Інформаційна боротьба другого покоління передбачає:

− створення атмосфери бездуховності й аморальності, негативного відношення до культурної спадщини ворога;

− маніпулювання національною свідомістю соціальних груп населення країни з ціллю створення політичної недовіри та хаосу;

− дестабілізація політичних відносин між партіями, об'єднаннями й рухами з метою провокації конфліктів, розпалення напруженості, підозрілості, загострення політичної боротьби, провокування репресій проти опозиції і навіть громадянської війни;

− зниження рівня інформаційного забезпечення органів влади й управління, інспірація помилкових управлінських рішень;

− дезінформація населення про роботу державних органів влади, підрив їхнього лідерства в очах громадян, дискредитація органів управління;

− підрив міжнародного авторитету держави, його співробітництва з іншими країнами;

− нанесення збитку життєво важливим інтересам держави в політичній, економічній, оборонній та інших сферах.[21]

Отже, у систему форм ведення інформаційної боротьби важливо включати інформаційні кампанії, операції, удари, акції, атаки. Звичайно, ці форми мають тісний взаємозв’язок і певну ієрархію.

Найнижчою формою інформаційної боротьби в такій системі є інформаційна атака, найвищою – інформаційна кампанія. Основу кожної з наведених форм інформаційної боротьби становлять інформаційні події, які плануються і проводяться системно й у визначеній сукупності утворюють інформаційну атаку, акцію чи удар.

Інформаційна подія – це елементарна короткочасна цілеспрямована інформаційна дія деструктивного характеру на об’єкт впливу в одному інформаційному напрямку. Інформаційна діяльність може бути як психологічною,

так і технічною. Перший напрямок спрямований на свідомість і підсвідомість людей. Другий – для комп'ютерів, телекомунікаційних систем, інформаційних ресурсів тощо, наприклад, несанкціонований доступ до електронної бази даних державного органу чи впровадження шкідливого програмного забезпечення в комп'ютерну мережу конкретного військового органу влади.

Отже, прикладом даного терміну може виступати ситуація, коли на площі Незалежності в Києві грав Гімн радянського союзу, збій в роботі державних банків та сайту Міністерства Оборони України – це все інформаційні події, запевняють фахівці. Інформаційні напади як і війна тривають вже близько восьми років, жертвами російської дезінформації стали не лише українці а й світова спільнота. Свою дезінформацію російські найманці розповсюджують для того, щоб дестабілізувати ситуацію всередині України. Вони поширюють неправдиву інформацію по сайтах, та соціальних мережах, аби залякати громадян, вплинути на їхню психіку та посіяти паніку на території країни.[22]

Інформаційна атака – це сукупність кількох взаємопов'язаних інформаційних заходів, які коротко спрямовані на один об'єкт впливу у певному інформаційному полі. Інформаційні атаки в більшості випадків носять технічний характер і спрямовані на конкретний інформаційний носій чи засіб, конкретну телекомунікаційну систему або управління. Інформаційні атаки можуть бути комп'ютерними (кібератаки), електронними, комбінованими тощо. За напруженістю вони можуть бути як вибірковими, так і масовими, але у всякому разі - прихованими і обмеженими в часі. При цьому інформаційні атаки психологічного характеру спрямовані проти певної особи чи конкретної групи людей.

Кібератаки, які відбувають станом на 1 травня 2022 року, приписують російській групі Killnet, яка працює по принципах хактивізму та спеціалізується на DDoS-атаках на країни, які, вони вважають, що підтримують Україну. Група здійснювала такі атаки на урядові веб-сайти в ЄС та на веб-інфраструктуру НАТО, а останніми днями атакувала веб-сайти урядових організацій Румунії.

DDoS-атака – це атака відмови в обслуговуванні, спрямована на відключення сайту або сервера. Під час такої атаки багато пристроїв, заражених вірусом,

одночасно починають відвідувати один і той же сайт, він не встигає обробити вхідне навантаження і перестає відкриватися або працює дуже повільно.[23]

Інформаційний удар – це комплекс цілісності зазделегідь скоординованих інформаційних атак, на певну кількість важливих частин державного і військового управління противника, з метою вибити з колії ворога.

Інформаційні удари більшості випадках проводяться, для того, щоб мати більшу перевагу на інформаційному рівні над супротивником. Фактично таким чином будуть проводитись не інформаційно-психологічні напади, а інформаційні операції, тому вважати інформаційну-психологічну операцію окремою формою інформаційної війни не потрібно.

Інформаційна операція – це сукупність вибраних та пов'язаних між собою завдань, ціль, об'єктів впливу і моментом інформаційних нападів, акцій, протистоянь, та ударів які можуть відбуватися як поступово так і одночасно в одній певній частині функціонування країни. Під час мирного стану, метою даних інформаційних операцій може бути також ефект на морально-психологічний стан вищого національного керівництва держави противника і важливих соціальних груп населення щоб схилити їх до прийняття рішень тих які потрібні ворогу.

Прикладом інформаційної операції є дії, які відбувались на території Маріуполя, станом на березень 2022 року. А саме – це повідомлення від міської ради Маріуполя, про те що окупанти проводять насильницьку-примусову евакуацію жителів міста на територію Російської Федерації, і незаконно вивозять людей з Лівобережного району міста з різних сховищ в російські міста, забирають у людей документи, проводять через так звані «фільтраційні табори», де змушують працювати на різних заводах Російської Федерації. Радник Міністра внутрішніх справ України Вадим Денисенко, сказав що те що робить Російська Федерація, це виключно з точки зору телевізійної картинки, тому він зауважив що це насамперед інформаційна операція.[24]

Об'єктами інформаційних операцій виступають у більшості населення країни ворога, певні соціальні спільноти, люди які мають вплив на прийняття державних рішень, керівництво, і також країни які є сусідами певної держави.

Інформаційна кампанія – це сполучення взаємопов'язаних інформаційно-психологічних засобів, які мають на меті лише один певний об'єкт ефекту в інформаційному напрямку і відбуваються вони в якийсь період часу. За деякими аспектами інформаційна кампанія подібно до інформаційної атаки але вона має більший обсяг та тривалість дії, психологічно характерна та зосереджена проти індивіда та населення. Головними об'єктами інформаційних атак виступають, національні діячі конкурентної держави, окремі соціальні спільноти та інші.[20]

Говорячи про види інформаційних війн, науковці виділяють основні з них, отже:

- Психологічна війна.

Головним напрямом діяльності психологічної війни є: завдання психологічної шкоди, виготовлення рекомендацій для реалізації психологічних атак, дослідження психології противника. У сучасному світі політика психологічної війни є всеосяжним напрямком діяльності більшості країн, Так, за приклад ми можемо взяти конгрес США, який ухвалив закон «Сміта-Мукда» ще в 1948 році, що надав уряду право створювати пропагандивні служби для вторгнення у справи інших міжнародних країн. Згідно з даним законом був створений апарат психологічної війни до якого увійшли: Пентагон, Управління міжнародного розвитку, ряд інформаційних агенцій, Корпус миру радіостанція «Голос Америки» та різні недержавні організації.

Отже, можна виділити головні ознаки сучасної психологічної війни:

−загальність, вторгнення в усі напрямки життя(в соціальні стосунки, економіку, дипломатію, культуру, тощо)

−широкомасштабність, впливовий ефект на всі сфери функціонування противника, збройних сил, громадян, сусідів та нейтральних держав.

−впорядкованість, створення різних органів психологічної війни та чітке зосередження на їхніх зусиль та напрямів діяльності.

−технізація, широкомасштабне застосування здобутків в сфері науки й техніки в плані вивчення змісту, способів та засобів психологічної війни та форми їх реалізації.

У термінологічному словнику можна знайти таке визначення психологічної війни: «Психологічна війна – це планомірне використання державою в період війни або надзвичайного стану засобів пропаганди з метою впливу на думки, емоції, позиції та поведінку організованих ворожих, нейтральних і дружніх груп таким чином, щоб сприяти досягненню своєї національної політики та визначених цілей».[25]

Об'єктами психологічної війни виступають: збройні сили та громадяни певної країни, дружні, нейтральні та ворожі держави.

Характер психологічної операції:

- оборонний, утвердження власного морального духу у разі попадання в полон та знешкодження дій ворога.
- наступальний, навіяти противнику сумнівів на рахунок певних планів та власних дій.

Засобом психологічної атаки виступають: пропаганда, розповсюдження неправдивої інформації, провокації, випуск фальшивих грошей, документів, поширення чуток, створення хаосу, саботаж, терор тощо.

Якщо аналізувати пропаганду як засіб психологічної атаки, то з аналізу українських інфо-продуктів на розповсюдження російської дезінформації. Російська Федерація використовує плітки як історії про «розпилювання гуманітарних» та корупційних схем. Тобто, спроба показати, як щось у влади не іде по плану. Наприклад, розповіді про те, як хтось не отримував соціальну виплату чи спроби підбурити до зради. Це включає спекуляції щодо мобілізації. Владі потрібно набагато чіткіше вибудовувати комунікацію, тому що повідомлення в стилі «сусідка сестри моєї дружини розповідала, як її сина спіймали посеред вулиці і відправили на війну» дуже шкідливо.

«Краще мир на будь-яких умовах, ніж активні воєнні дії» таке повідомлення було записано в групі телеграм-каналів Кремля з початку вторгнення. Проте зі зростанням кількості жертв серед мирного населення пропагандисти все частіше намагаються переконати українців, що Україні не потрібен Крим чи Донбас, якщо будуть гинути стільки людей.[26]

На рахунок російських провокацій є достатня кількість прикладів, так російські літаки атакували білоруську територію на кордоні з Україною 11 березня 2022 року, імовірно, щоб втягнути Білорусь у війну, повідомили в ВПС України. Штурмові літаки, які летіли в Україну з Білорусі, бомбили українську територію, а потім завдали авіаударів по білоруській території. Такий напад і дії ворога на населені пункти в Білорусі є свідомою провокацією для втягнення збройних сил Білорусі у війну з Україною, переконані в Києві.

Зокрема, незадовго до нападу міністр оборони України Олексій Резніков заявив, що Російська Федерація «готує серію кривавих провокацій».[27]

Приклад саботажу можна навести, як головний директор заводу «Сітроен», який випускав одні з найкращих на той час вантажівок, знав, що якщо він відмовиться від співпраці, його просто замінить на більш підвладну людину до окупаційної влади. Тому він вирішив співпрацювати з окупантами та здійснювати диверсії. Директор та інші працівники заводу, які долучилися до диверсії, просто змінили конструкцію так званої «масляної штанги». Він показав, що рівень масла в двигуні був достатнім, хоча насправді він був менше мінімально необхідного. Це, у свою чергу, призвело до передчасного пошкодження двигуна.[28]

Метою психологічної війни є: впливовий ефект на почуття, емоції, розуміння ситуації, підсвідомість, волю, підривання власних поглядів, переконань та навіювання своїх цілей.

Таким чином, психологічну війну ми можемо вважати як планомірне використання державою та її установами засобів і заходів ідеологічної дезорієнтації та розкладання свідомості людей і груп людей з метою зниження їхньої ідейної, політичної, духовної та морально-психічної стійкості, спонукання до негативних дій або бездіяльності населення та особового складу армій інших держав як у воєнний, так і в мирний період.[25]

Психологічна війна полягає у використанні інформації всупереч людському розуму. М. Лібіцкі вважає що, існують чотири категорії психологічної війни[29]:

- операції проти національної волі;
- операції проти командування супротивника;

- операції проти воїнів;
- культурний конфлікт.

Операції проти національної волі мають дві складові частини. Вони можуть проводитись за принципом розпізнання друга в суб'єкті, шляхом прояви дружелюбних дій та допомоги, або взагалі навпаки показуючи всю серйозність дій та навіть за принципом шантажу. Саме ці методи віддавна є звичайним продовженням військових наступів, і відомі нам ще зі стародавніх часів. Як приклад ми можемо навести, передачу інформації в теперішньому часі з місця події, надання бажаної інформації та потрібного нам погляду на ситуацію, для того щоб викликати певні ефекти. Ці дії зводять до повної довіри ЗМІ та його використання.

Операції проти командування, зосереджені на тому, щоб дезінформувати та ввести в заблудження противника. М. Лібіцький вважає, що у суспільстві інструментом є начальство, шляхом якого воля політичного керівництва переступає підвладним. Гіпотетично, вони мусять бути емоційно стійкими та не зобов'язані приймати рішень чи змінювати отримані, але ефект на їхню свідомість може це змінити. Видозмінюючи реальність, змінюється одночасно й навколишнє середовище, де приймаються певні рішення, і також умови їх прийняття. Як приклад даної категорії психологічної війни можна навести розповсюдження неправдивої інформації про розміри або мету нападу.

Операції проти воїнів проводяться з тиском та емоційним впливом на підрозділи ворога. Головним завдання для цієї категорії є потрапити до підрозділів ворога з інформацією про можливий непередбачуваний розвиток подій та використання ре-сентиментів. Мова йде про радіопередачу, телетрансляцію і також про паперову форму.

Культурний конфлікт передбачає широкий спектр інструментів і етапів. Ця категорія психологічної війни полягатиме у протиставленні чи підтримці певного підходу в суспільстві, відчуття загрози чи миру. Не всі відрізняють збудження страху, образи чи ненависті від негайного культурного нападу. Крім того, це не нова концепція і не є похідною від технічного прогресу. Відмінності у підходах до власної культури, почуття національної самоідентифікації чи патріотизму, прихильність до

традицій, самосприйняття у міжнародному середовищі є одними з найважливіших факторів у культурному питанні. Це можна звести не тільки до експорту власної продукції, але й до принципів і цінностей.

Психологічні операції визнані однією з найдавніших нелетальних видів зброї в запасі суспільства. Їхні частини відомі нам ще з давніх часів (найкращий приклад – Троянська війна). С. Пін писав, ще до сторічь до нашої ери що кожна війна ґрунтується на обмані, дезінформації, і «найголовніше в нападі Дао на іншу країну – завоювати серця її громадян». Також, у XIII столітті Чингісхан вживав так звані «Агенти впливу» в штатах, які він хотів підпорядкувати чи контролювати, і проводили прогресивні дії психологічного тиску через емісарів.[30]

У вітчизняний час, щоб спонукати до появи у своїх громадян патріотичні погляди та переконання, зберегти у населення пріоритетність цілей державної політики, керівництво країни все це робить за допомогою ЗМІ. Але противник не дивлячись на це все має на меті навіяти громадянам та військовослужбовцям, ті ідеї та настрої, які потрібні саме йому. Наприклад, Радянський Союз розмістив свої війська та ракети поряд китайського кордону у В'єтнамі для психологічного тиску на населення та керівництва. США не один раз хотіли дійти до своїх політичних цілей шляхом, демонстрування своєї військової могутності, надсилаючи військово-морські групи в різні частини світу.

Також, для психологічного впливу в політичній сфері використовують дипломатичний вплив, який насамперед реалізується на керівництво держави. Саме так під час підготовки до операції в жовтні 1983 році у Гренаді США створили військово-політичний альянс східно-карибських країн, який засуджував політику керівництва Гренади. До цього союзу увійшли Антигуа і Барбуда, Домініка, Сент-Люсія, Сент-Вінсент та Гренадіни. Зародження цього союзу дозволило засобам масової інформації західних країн трактувати його заяву як результат загального невдоволення карибських країн політикою М. Бішопа та його кабінету.[31]

Ще прикладом психологічного тиску є:

Російські солдати почали чергову психологічну гру, заявивши, що зробили все, щоб вирішити продовольчу проблему, а тепер все залежить тільки від України.

90% українського експорту продовольства здійснюється морем, яке зараз контролюють російські кораблі та підводні човни.

Російська Федерація готова пропустити продовольчі кораблі, якщо Україна розмінує прибережну зону. Російська Федерація мовчить про гарантії, що не нападе з моря.

Це маніпуляція, адже російські пропагандисти поширюють на Заході звинувачення на адресу України та очікують підтримки від країн, залежних від українського зерна.

- Мережева війна

На думку військових аналітиків, поточні та майбутні війни будуть ще більше розвиватись в мережевому напрямку. Термін «мережева війна» – це новий якісний етап розуміння цілі та завдань сучасної війни, збройних атак. Мережні війни в більшості отримують перемогу не військовими засобами, а мережевими організаціями. Однак цілі мережевих воєн залишаються такими ж, як і у звичайній, класичній війні: перемогти ворога, захопити його ресурси, встановити прямий контроль над його територією, над його найважливішими районами.

У мережевій війні ворожа мережа охоплює ворога з усіх сторін. Такі явища війни, як звичайна партизанська війна, диверсії, дезінформація, провокації та заворушення, зараз наростають і стають новою формою мережевої війни. У мережевій війні країна стикається з діями ворога у вигляді зграї, здавалося б, не пов’язаних між собою дій (провокації, дезінформації, дипломатичні демарші), дій фондів, комітетів із захисту певних цінностей, злочинні угруповання, політичні рухи, телеканали, Інтернет-сайти.

Об'єктами мережевої найчастіше виступає керівництво країни, громадяни, армія, МВС, еліта суспільства. У цей список можна включити дипломатію, пропагандистські та психологічні кампанії, політичну та культурну шкоду, шарлатанство чи втручання в роботу ЗМІ, запровадження комп’ютерних мереж або баз даних, підтримку дисидентських та опозиційних рухів. Мережева війна – це всеосяжний конфлікт, який розвивається в усіх галузях, у ряді економічних, політичних, соціальних і військових аспектів. Форми мережевих воєн можуть бути різними: від конфлікту між державами до конфлікту між державними та недержавними структурами.[32]

Характерною ознакою інформаційно-мережевих воєн є відсутність жорсткої ієрархії в мережевій структурі загарбника. Це пояснюється його неоднорідністю, що виражається у значній автономії державних і недержавних елементів цієї структури, в якій немає чітких вертикалей з'єднання. У мережевій структурі суб'єкт не керується наказами згори, а їхні мотиви та загальні правила в плані загальних ідеологічних уявлень про соціальне середовище, чиї інтереси воно захищає. Звідси і відсутність ієрархії, побудови мережі та організації взаємодії між цими елементами, не дозволяє чітко встановити існування і діяльності структур такого типу. Джерело енергії, можна сказати «мережне паливо» – це інформація, яка активізує «робочий орган» – певні соціальні групи та групи населення, а своєрідним «вогнем» є хаби – сервери глобальних соціальних мереж, до яких перш за все включається Facebook і Twitter. Тому недаремно в політології з'явилося таке поняття, як «революція T&F» [33].

Отже, прикладами мережевих війн є дії альтерглобалістів, радикальні борці за екологію, азійських тріад руху «Хезболла», мексиканські запатисти чи сербська організація «Отпор» тощо.

Хезболла – це партія Бога або партія Аллаха, також ліванська шиїтська парамілітарна ісламістська організація і політична партія. Рух Хезболли був започаткований у відповідь на ізраїльську окупацію Лівану у 1982 році за допомогою прихильників Аятоли Хоменеї. Хезболла бачить Ізраїль як «нелегальне узурпаторське угрупування, засноване на зрадливості, різанинах і ілюзіях». Здебільшого вона підтримується шиїтським населенням Лівану, та є однією з двох впливових шиїтських організацій Лівану.[34]

Отпор – це є непартійний колективний молодіжний рух у Сербії, на основі якого лежать принципи ненасильницького спротиву. Відіграв вирішальну роль в поваленні режиму Слободана Мілошевича в жовтні 2000 року. На вершині своєї активності Отпор налічував понад 70 000 учасників. Отпор був утворений 10 жовтня 1998 року у відповідь на репресивні закони про університети та ЗМІ введені на початку цього року, коли уряд Сербії очолював лояльний Мілошевичу Мірко Мар'янович. На початку діяльності Отпор існував лише в рамках Белградського університету.[35]

Альтерглобалізм – це соціальний рух ідеологія якого близька до класичного антиглобалізму, але в підтримці якого лежать деякі аспекти глобалізації перш за все світову інтеграцію, відкидаючи заперечення, що значення демократії, економічного правосуддя, екологічного захисту і прав людини повинні стояти попереду економічних турбот.[36]

- Ідеологічна диверсія

Однією з основних форм підривної діяльності розвідувальних та інших спецслужб імперіалістичних держав, їх ідеологічних і пропагандистських центрів є агітаційно-пропагандистські або розвідувально-організаційні дії. Заходи та операції, що здійснюються спеціальними силами і методами та спрямовані на натхнення, стимулювання та використання антисоціалістичних тенденцій, процесів і сил з метою підриву чи послаблення державного і соціального ладу в кожній окремій соціалістичній країні, а також єдності громади.

Кінцевою метою ідеологічного саботажу є прагнення ліквідувати соціальні та державні системи соціалістичних країн або послабити їх, щоб вони не могли протистояти збройній агресії імперіалізму. Ідеологічний саботаж зачіпає всі сфери суспільного життя соціалістичних країн – ідеологію, політику, економіку, мораль, право, культуру і науку. Але, надихаючи й стимулюючи антисоціалістичні тенденції та процеси в усіх цих сферах, ворожі спецслужби підпорядковуються політичним цілям – цілям підриву й ослаблення соціалістичної держави. Тому в будь-якому акті ідеологічного саботажу необхідно виявити політично підривні цілі, які часто ретельно маскуються. Ідеологічний саботаж – незаконна діяльність, пов'язана з втручанням у внутрішні справи соціалістичних країн.[37]

«Празька весна» виступає основним прикладом ідеологічної диверсії. Головним пропагандистським мотивом введення військ стало твердження, нібито до Чехословаччини вже готові ввірватись війська НАТО, в більшості американські і західнонімецькі. Це була пряма брехня, тому що перед тим як вводити війська Леонід Брежнєв провів бесіду з президентом США Ліндоном Джонсоном і одержав від нього гарантію того, що ніякої військової відповіді на радянську інтервенцію до Чехословаччини з боку Америки і НАТО не буде. Більшість радянських людей, що не

мали доступу до певних джерел інформації, вірили цій маячні. Звісно, громада більш того не лише з числа опозиціонерів, знала всю фантастичність положень про загрозу Чехословаччині з боку Північноатлантичного союзу. Але більшість радянських громадян були впевнені, що Радянський Союз вкотре продемонстрував свою силу і не дозволив піти з-під свого контролю одній з найважливіших держав у центрі Європи.[38]

−Семантична війна

Семантична війна – це війна за право давати явищам імена. Це війна наративів, війна героїв, війна назв. І саме тому важливо, кому, яким героям стоять пам'ятники, якими іменами називають вулиці.

Головною метою семантичної війни це породжувати нові дискурси. Отже, семантична війна – це війна дискурсів на рівні ментальних установок.

Семантична війна є необхідною умовою початку семантичної революції, яка закріплює нові психічні установки в суспільстві і тим самим зміцнює інтелектуальні позиції мислячих людей, а також створює основу для стійкої переваги громадян з цими психічними установками.[39]

Чудовим прикладом семантичної війни є святкування перемоги над нацизмом у Другій світовій війні. Ось є два чітко окреслених наративи: «можем повторить» та «ніколи знову». Ці два детально опрацьовані й вбирають у себе значну кількість інших фрагментів великої історії. Кожен громадянин, який святкує завершення Другої світової, чи то як День перемоги, чи то як День пам'яті, своїми власними думками, емоціями й діями скріплює, надає більше переваги той чи інший наратив. Хоче чи не хоче, але займає своє місце в окопах семантичної війни.

З цим поняттям історії беремо за приклад процеси в Україні і навколо неї, і бачимо війну історичних аспектів як складову української війни за незалежність.

У частину цієї війни входить історичний рефрейминг, що, за словами одного з основних російських стратегів Сєргєя Переслєгіна, робить історію «абсолютною зброєю, яка викреслює супротивника з реальності: замість чергового покоління супротивника народжується покоління, що належить країні, яка приватизувала

історичний процес». Таким чином ведеться семантична війна, за право давати явищам і подіям імена – є найвищим рівнем війни.[40]

Також до видів інформаційного протистояння ми ще можемо віднести:

- Інформаційна війна в інтернеті – надаються різні неправдиві фактори для залякування, також розповсюдження обманливої інформації.
- Психологічні операції – підбір і подача певної інформації, яка звучить як контраргумент на настрої, що існують в суспільстві.
- Дезінформація – розповсюдження фейкової інформації, щоб збити з шляху ворога.
- Руйнування – фізичне знищення або блокування інтернет ресурсів, які є важливими для противника.
- Заходи безпеки – посилення охорони своїх ресурсів з метою збереження планів і намірів.
- Прямі інформаційні атаки – змішання помилкової і правдивої інформації

До видів інформаційної зброї відноситься: введення нової інформації, введення спотвореної інформації, запровадження нових правил опрацювання інформації[41].

Головною технологією інформаційної війни, зазначає науковець Г. Почепцов, є відсутність інформації, що моментально закривається чутками. Також він наголошує на вірогідності існування певного закону про можливості вакууму інформації: коли її не дають офіційні джерела, вона тут же з'являється в неофіційних каналах [42].

М. Лібіцькі вважає, що інформаційна війна, це не окрема техніка ведення війни, а більш глобальніша концепція. За його класифікацією, вона має сім основних форм[29]:

−війна на рівні командування і контролю (Command-andControl Warfare);

−війна на підставі розвідки (Intelligence-based Warfare);

−електронна війна (Electronic Warfare);

−психологічна війна (Psychological Warfare);

−хакерська війна („Hacker" Warfare);

−війна на базі економічної інформації (Economic Information Warfare);

−кібервійна (Cyberwarfare).

2.2 Методи та способи ведення інформаційних війн

На сьогоднішній день бачимо, що саме Інтернет все більше і більше набирає силу агітаційного та пропагандистського сектору, що відрізняється чітко вираженою агресивністю. Також великий вплив на свідомість громадян дають традиційні ЗМІ які все більше працюють з інтернет-ресурсами як джерелами інформації. Інформаційна війна має на меті управління процесом зміни свідомості населення, їх оцінки ситуації, ставлення до суспільства і країни, небезпечним для громадян є втрата власної волі а для самої країни – її суверенітету.

У різний час змінюється інтенсивність використання тих чи інших методів впливу, а також рівень його організації. Дивлячись на методи інформаційного тиску, можемо сказати, що впродовж століть вони залишаються незмінними, але якщо подивитись з іншої сторони, то бачимо, що методи інформаційного впливу значно вдосконалились та змінили канали передачі інформації. Щоб більш детальніше розглянути дані методи ведення інформаційної війни пропонуємо поділити історію інформаційного конфлікту на три періоди.

Перший період започаткування інформаційного тиску охоплює Античність, Середньовіччя і частково Новий час. Впродовж даного періоду методи та способи ведення інформаційної війни залишались незмінними, пізнаючи лише несуттєвих видозмін.

На другий період інформаційного протистояння випадають чіткі перетворення і споріднені з значним збільшенням впливу інформації в суспільному житті. Це можемо спостерігати в часи буржуазних революцій у Європі, від середині XVII ст., закінчуючи роками другої світовою війною. У даний період відбуваються серйозні зміни в організації інформаційної війни, розвитку її методів та форм, зростає значення інформаційних атак, це відзначається зростанням ролі цієї боротьби як ефективного інструменту вирішення військових, політичних чи економічних проблем.

Третій період ще більше посилює значення інформаційного впливу на суспільство в цілому. За допомогою інструментом керування суспільством, інформаційне протистояння перетворюється на один з головних методів досягнення цілі. Відповідно змінюється рівень наукового та матеріально-технічного забезпечення такого типу протистояння. Перехід до цього періоду підготовлений і зумовлений певним рівнем розвитку інформаційних технологій. Сучасні інформаційні технології базуються на досягненнях комп'ютерної техніки та комунікацій. Швидкий розвиток комп'ютерних та інформаційних технологій дав поштовх до розвитку суспільства, відомого під назвою «інформаційне суспільство».[43]

Досліджуючи джерела інформації можемо навести декілька прикладів підготовки до інформаційної війни та самі способи ведення цих війн.

Отже, першим прикладом є ігри «Бій без поля бою – війна в XXI ст.» які відбувались в 1995 році працівниками корпорації RAND, участь брали вказівні фахівці США в сфері комп'ютерної безпеки із корпорацій, державних організацій та Міністерства оборони США. У цих іграх фахівці відробляли стратегічний захист США, при застосуванні противником методів інформаційної війни. В якості потенційного ворога розглядався Іран.

Якщо брати до уваги більш новітні та сучасніші інформаційні війни, зосередимо увагу на Російській Федерації, Ірану, Китаю, Саудівській Аравії які більше семи років ведуть інформаційну війну не лише з Україною а й з іншими країнами та альянсами.

Основними методами ведення інформаційної війни вони використовують психологічні атаки, створюють фейковий контент і проводять фальшиву активність.

– Іран налаштовував Ємен проти Саудівської Аравії. Єменські сайти, які були підроблені та розміщені в Ірані, видавали публікації з осудженням дій Саудівської Аравії в Ємені. Наприклад, «Yemeh Press Agency» опублікували список «саудівських злочинів проти єменців за останню добу».

– Російська Федерація мала на меті розпалити сутички між Україною та Польщею, у 2013 році, коли завершились протести на Майдані, на польських

просторах інтернету гуляв фейк антиукраїнської пропаганди. У цих статтях вони підтримували російські дії та їхній уряд на певних інтернет-сайтах, таких як форум російсько-польського радіо Sputnik Polska. Sputnik – російське державне інформаційне агентство, яке працює в багатьох країнах. Російська пропаганда поширює брехню, що Польща має зрадницький намір стати на бік Росії та захопити Західну Україну. Відео з таким повідомленням поширює прокремлівський блогер Юрій Подоляк. Він також стверджує, що після окупації частини Західної України Польща розпочне денацифікацію українського населення. Натомість 20 травня 2022 року президент Польщі Анджей Дуда заявив, що вважатиме перемогу України з повним відновленням територіальної цілісності найкращим завершенням війни Росії проти України. Це ще раз підтверджує добросусідські відносини між Польщею та Україною.

Раніше в Російській Федерації закликали поставити Польщу на перше місце за «денацифікацію» після України. Це реакція на останні заяви прем'єр-міністра Матеуша Моравецького щодо ідеології «русского мира».[44]

– У квітні 2016 року в Нідерландах пройшов референдум щодо торговельної угоди між Європейським Союзом та Україною. Раніше російські ЗМІ оприлюднили фейкову історію про українського військового, який збив у Донецькій області «Боїнг 777», у результаті чого загинули 193 голландця. Інтернет-видання Bellingcat дослідили цю інформацію і виявили схожий негативний контент на сайтах інших країн. Наприклад, YouTube-канал «Патріот» було опублікувано відео «Азовці звернулися до Нідерландів з проханням провести референдум щодо асоціації Україна-ЄС». На відео шість україномовних «солдатів» нібито спалюють прапор Нідерландів.

– Також Російська Федерація намагалася налаштувати Литву проти НАТО, її метою було пошкодити представлення та ставлення в цілому до НАТО не лише в Литві, а й в інших країнах Балтії, які допускають операції НАТО. Вміст мав виглядати так, ніби він був створений у цих країнах. Наприклад, у статті хакерів сказано, що навчання НАТО в Литві були спрямовані на окупацію Білорусі.

– У Бразилії з серпня по вересень 2018 року через Twitter, Facebook і Whatsapp розповсюджувалась фейкова інформація, яка мала значний ефект на бразильських виборців. Аналітики відокремили спільноту з 232 профілів, які писали про тодішнього кандидата в президенти Жайро Балсанарі та президента Бразилії Луїса Інасіу Лулу да Сілву, і публікували фейкові новини. Лише за місяць у Twitter було написано 8185 дописів на португальські політичні теми.[45]

Отже, беручи до уваги всі ці інформаційні атаки ми можемо побачити який великий вплив має інформація. Аналізуючи всі методи, які були задіяні в наведених вище інформаційних війн, бачимо, що основною зброєю є психологічний тиск, який впливає на бачення та думку суспільства через інтернет ресурси. У даній війні немає вікових категорій, адже кожна людина яка має доступ до інтернету може піддатись впливу інформаційних атак, і не хотячи цього може стати посередником в цій війні.

Психологічна ізоляція об'єкта включає заходи в політичній, економічній та військовій сферах.

У політичній сфері це може бути дипломатичний вплив на керівництво сусідніх країн. Так, під час підготовки до операції в Гренаді в жовтні 1983 року США створили військово-політичний альянс у Східно-Карибському басейні, який рішуче засудив політику керівництва Гренади. До цього союзу увійшли Антигуа і Барбуда, Домініка, Сент-Люсія, Сент-Вінсент і Гренадіни. Поява цього альянсу дозволила західним ЗМІ інтерпретувати його появу як результат загального невдоволення країн Карибського басейну політикою Бішопа та його кабінету.

Психологічна ізоляція у військовій сфері є переважною демонстрацією рішучості використовувати збройні сили для вирішення кризи.

Другим способом інформаційно-психологічного впливу, який активно використовується для тиску на населення інших країн, є дезінформація. Він використовується для того, щоб якнайшвидше переконати населення та світову спільноту у необхідності насильницького вирішення проблеми.

Важливим аспектом інформаційного конфлікту в цілому та психологічних операцій зокрема є вплив на політичних і військових керівників, а також на керівників (видатних представників) засобів масової інформації, культури і мистецтва

противника. У зв'язку з цим, наприклад, у США особлива увага приділяється створенню колективних та індивідуальних моделей поведінки вищого і середнього керівництва та військового керівництва, створенню так званих психологічних портретів лідерів.

На оперативному рівні проводяться інформаційно-психологічні операції для забезпечення успіху операції або походу в цілому, вирішення основних завдань, операції. Їхня мета – впливати на системи зв’язку, матеріально-технічного забезпечення та бойового управління збройними силами, одночасно захищаючи подібні системи як власних збройних сил, так і збройних сил союзників.

Інформаційно-психологічні операції проводяться на тактичному рівні для забезпечення вирішення тактичних завдань. Зазвичай вони зосереджені на інформаційних системах та інформації, пов’язаній з бойовим управлінням, розвідкою, зв’язком і безпосередньо забезпечують бойові дії з підрозділів і з’єднань противника. При цьому вживаються заходи щодо захисту власних і суміжних систем.[46]

До основних засобів інформаційної війни належать такі інформаційні заходи як засоби військово-політичної дезорієнтації противника; неправдива інформація про власні ресурси; дії, зосереджені на знищення або блокування каналів передачі даних з метою дезорієнтації, створення атмосфери напруженості в суспільстві від постійного очікування мітингів та впливу на масову свідомість населення з метою деморалізації та поширення паніки. Постійне наростання інформаційних витоків унеможливлює їх контроль для країни. Тому головним завданням у протистоянні в інформаційній війні є не контроль над потоком інформації, як слушно зазначає О. Дугін [47], контроль алгоритму руху інформації для її розшифровки і тим самим убезпечення суспільства та його управління.

До головних методів ведення інформаційно-психологічної війни відносимо такі аспекти як пропаганду, поширення чуток, провокації, дезінформування, психологічний тиск, диверсифікацію суспільної свідомості тощо.

Найпоширенішим методом інформаційної війни є пропаганда, яка передбачає поширення політичних, релігійних, філософських, наукових чи інших сфер шляхом

передачі громадянам різноманітних аргументів, правдивих чи неправдивих фактів, чуток чи відвертої брехні з метою маніпулювання суспільною свідомістю.

Г. Лассавелла, був одним з перших, хто проаналізував в своїх працях роль пропаганди, він визначив пропаганду як особливий вид зброї, що має можливість впливати на психічний стан ворога. Автор виділяє такі основні цілі пропаганди: розгортання ненависті до противника; підтримання дружелюбних відносин з сусідніми країнами та союзниками; тримати добрі відносини з нейтральними державами і старатись налагоджувати з ними режим співпраці;[48]

Також, звертаємо увагу на думку французького соціолога Жака Еллюля, який трактує пропаганду в різних видах, тобто вертикальну та горизонтальну. Вертикальну пропаганду він розуміє як класичний варіант, так як ми всі її розуміємо, інформаційна течія згори до низу з нейтральним реагуванням громади. А на рахунок горизонтальної пропаганди, то Ж. Еллюль вважає її своїм новим винаходом. Назва «горизонтальна» походить від реалізації її в певній соціальній групі, а не вихід згори. Інформація, яка надходить вважається достовірною тому що, всі учасники є рівними і серед них немає певного лідера. Також автор даного трактування розрізняє два різновида горизонтальної пропаганди: китайська та американська, які зумовлені особливостями групової динаміки.

У китайському варіанті не потребується висловлення своєї думки від членів групи. А в американському варіанті наоборот, від групової динаміки вимагається активність та проявлення особами власної позиції. Горизонтальна пропаганда потребує значної самоорганізації людей, а вертикальна вимагає великого апарату масових комунікацій. До речі, автор пояснює пропаганду, як ірраціональну форму існування деяких думок, а саму інформацію він називає раціональною. Багато в чому він накладає горизонтальну пропаганду на актуальний сьогодні феномен соціальних мереж. Ще Ж. Еллюль виділяє політичну та соціальну пропаганду. Про політичну можна сказати, що це техніка впливу на громадян зі сторони держави, партій, та інших владних кампаній.

Соціологічна – це як живе суспільство, види поведінки, звичаї та традиції, які є принципами в певному суспільстві. Ж. Еллюль говорить, що соціологічна пропаганда

є складнішою для розуміння, тому що вона є непомітною. Якщо соціологічна пропаганда є ідеєю пробивання в свідомість, дякуючи існуючим політичним, економічним, культурологічним, соціологічним аспектам, то політична пропаганда є цілenаправленою, спрямованою для розповсюдження певних планів.

На перший погляд різниця між вертикальною та горизонтальною пропагандою, політичною та соціологічною, може здатися несуттєвою. Але між ними все ж таки є значні відмінності. Вертикальна і горизонтальна пропаганда пов'язана з напрямком комунікації, що відображає ієрархію суспільства. У разі розмежування політичної та соціологічної пропаганди увага приділяється каналам поширення інформації, коли це може бути будь-який інститут суспільства.[49]

Отже, можна виділити основні методи пропаганди: формування в масовій свідомості образу жертви з особи, яка причетна до неї, яка насправді є злочинцем, перекладання відповідальності та приписування власних злочинів ворогу, ігнорування фактів та таврування незгодних з пропагандою.

«Сендвіч з дезінформацією» – це найпоширеніша технологія пропаганди, яка полягає в нашаруванні правдивої та неправдивої інформації в повідомленні, тобто. створення «бутерброда» з реальних фактів і фальсифікацій, останнього «шару», в якому пропонується рішення проблеми. До прикладу можна віднести таку пропаганду російських ЗМІ:

«Не всі українці в Україні погані, але є націоналісти та бандерівці. Бандерівці погані, 8 років бомбили Донбас. Але ми визволимо правильних українців від бандерівців, тому ми повинні бомбити поганих українців, особливо на Донбасі. А як знешкодити Бандеру іншим способом? Хоча ми не будемо робити це «як Бандера», але ми запустимо високоточні ракети, щоб уникнути мирних жителів і вільних добрих українців.»

Такий «підроблений бутерброд» можна нейтралізувати «бутербродом правди». Необхідно повідомити, що сталося насправді, розкрити підробку, коротко пояснити неправдиві факти і знову сказати правду.

У більшості науковці, пропаганду зображають в поганому значені, і це так і є. Пропаганда за авторитарним режимом відіграє деструктивну функцію, тому що

джерела інформації зумовлені державою, а сама пропаганда стає формою спілкування з навколишніми. Але, не забуваємо, що саме пропаганда не є обов'язковим видом поширення корпоративних та упереджених позицій. Пропаганда також може бути і позитивним інформаційним аспектом, що доносить суспільству важливу інформацію, розміщує демократичні принципи, патріотизм, єдність громадян тощо.

Слід зазначити, що моментами діалог може бути недоречним. У політичній сфері є багато випадків, коли владі потрібно просто повідомляти, переконувати суспільство, не чекаючи від них зворотного зв'язку. Часто, при вирішенні якогось конфлікту позитивним результатом є не інформування суспільства, це допомагає зберегти спокійну атмосферу в соціальній аудиторії. Але з іншого боку, спираючись на позицію, що населення повинно бути проінформоване всім, ЗМІ розпалюють політичні пристрасті і дезорієнтують ситуацію. У похожих ситуаціях застосування пропагандистських технік цілком потрібно та доречно.

На думку дослідника В. Петрика, дезінформація та маніпулювання певною інформацією здійснюється такими шляхами як:

−необ'єктивний виклад фактів (певної інформації, що перебуває в упередженому повідомленні фактів чи іншої інформації про події шляхом спеціально відібраних певних даних; в більшості, за допомогою даного методу спеціально виробленої інформації , до постійно зростаючої напруги);

−неправда висвітлена в певному контексті як правда (виникає за допомогою надання достовірної інформації в викривленому вигляді або в ситуації, коли вона сприймається об'єктом як неправдива; і так в підсумку суб'єкт дійсно знає правдиву інформацію про плани або конкретні дії протилежної сторони, але сприймає її неадекватно, не готова протистояти негативним впливам);

−нейтральна дезінформація (містить в собі використання комбінування точної інформації з дезінформацією);

−«чорна» дезінформація (з використанням переважно неправдивої інформації) [50].

Поширеним методом, який впливає на свідомість людей є психологічний тиск. Використання цього методу включає в себе вимагання, репресії, розповсюдження на сайтах інформації про можливі чи уявні ризики та небезпеки, втілення терористичних актів та підривів. У довоєнній практиці популярним був телефонний тероризм, інакше кажучи телефонували з інформацією, що нібито замінували станції або різні громадські місця. До головних технік тиску можемо віднести шахрайство, політичні ігри та рекламні кампанії, провокації, чутки, дезінформація.

Провокацію можна віднести до ряду найпопулярніших методів ведення сучасних інформаційних воєн, яка схиляє ворога до збиткових для нього дій.

Провокація – це цілеспрямований стимул для почуттів і емоцій. Провокатор передбачає дії людини яку провокує і хоче отримати те що входить в його плани, матеріальні або просто психологічна насолода, шляхом стимулювання до непродуманих дій та слів. З латинської provocation перекладається як «виклик», виклик для тих, на кого спрямована провокація.

Існують два види провокації:

Явна. Явну провокацію визначити дуже просто. Людина, якій потрібно щось від вас, звертає на вас більше уваги: хвалить, лестить, захоплюється або відкрито провокує, може образити, використати цькування, сваритися з кимось. У будь-якому разі це може викликати надзвичайні емоції, негативні або позитивні. Під впливом таких почуттів можна легко втратити самовладання, і цей розвиток подій розробив провокатор.

Неявна. Неявну провокацію зрозуміти набагато важче. Можна сказати, що це маніпуляція. Для досягнення поставленої мети провокатор намагається завоювати довіру, одягає маску доброзичливості і завжди готовий прийти на допомогу. Ви хочете віддячити йому так же само, так ви розкриваєтеся і видаєте потрібну інформацію або робите послугу, яка зашкодить вам.[51]

Чутки – це досить особлива технологія інформаційної війни. Професор Г. Почепцов зауважив, що часто відсутність точної інформації миттєво компенсували чутками. Шляхом розповсюдження чуток, люди так проявляють свою форму самовираженням, своє ставлення, оцінюючи те що трапляється з ними та круком них

у середовищі. Чутки мають спосіб впливу та формування громадської думки і показують психологічний стан населення в певний відрізок часу. Чутки також, якщо започатковані на точній інформації або фактах, які виплили з офіційного джерела, всеодно інформацію подають у спотвореному вигляді, тому що ця інформація, що міститься і циркуляє в чутках, дефілює через свідомість громадян, свідомо чи мимоволі викривляє її на шляху. Вчені які спеціалізуються в цій сфері, пояснюють це тим, що коли суспільство оточено чимось новим та нерозбірливим, але коли це є важливим для них, то вони в пошуках тої інформації яка потішить їх свідомість за заспокоїть. Також можна сказати, що чим довше тривають чутки, тим менш надійними вони стають.[52]

Раніше війни відбувались з метою фізичного знищення. Зараз критичне мислення руйнується. Світ переживає цифрову трансформацію – процес змін бізнесу за допомогою технологій, але як ми може бачити змінюється не тільки бізнес. Незмінним протягом століть залишається війна.

Звісно, пропаганда завжди маскувалася. У 1940 роках США винайшли Капітана Америку, щоб підвищити свою військову репутацію та заохотити молодих людей приєднатися до збройних сил. А якщо вернутись ще на декілька років назад – в період Першої світової війни – Британія сповна скористалася брехливими розповідями про звірства німецьких солдатів, наприклад, про те, що вони переробляють трупи співвітчизників, щоб нагодувати свиней.

Але оскільки зараз майже кожен житель планети має доступ до Інтернету, отже і можливість мати ефект на наші думки та дії набагато більша. Інформаційні нападники зараз не тільки говорять про ворога, вони формують інше бачення світу, замінюючи реальність таким навмисним обманом, що його майже неможливо відрізнити від правди.

РОЗДІЛ 3. ІНФОРМАЦІЙНА ВІЙНА РОСІЇ З УКРАЇНОЮ

3.1. Основні моделі інформаційних війн

Вплив інформаційної війни на різні сфери: політичні, соціальні, економічні, на всі рівні управління та соціального устрою значно збільшився. Суть інформаційної війни полягає в тому, щоб мати під впливом велику кількість суспільства, їхню свідомість – це надає змогу контролювати і змушувати людей діяти певним чином, інколи проти власних інтересів.

Події, які відбуваються в сучасному світі, дають можливість бачити, який інформаційний вплив на свідомість людей має руйнівний характер. Інформаційний зміст, який ми бачимо щоденно у ЗМІ, має в собі емоційне забарвлення, перед яким громадяни не можуть встояти. Чим більше зростає вплив ЗМІ на свідомість громадян, тим більша йде загроза на населення. Моделі, які застосовуються в інформаційній війні, все більше переплітаються, що плутає свідомість людей де правда, а де її немає.

Те, який результат дає інформаційна війна та насамперед її дії, залежить від того яку модель впливу вона використовує.

Тлумачення моделей інформаційної війни західних і вітчизняних вчених мають істотні відмінності, оскільки наукова база перших багатша за другу. Саме тому, на теперішньому етапі розвитку європейські політології більше уваги приділяється кібертехнологіям інформаційної війни, а на пострадянському просторі – військово-технічним чи психологічним технологіям інформаційної війни. Однак, проведення спеціальних інформаційних операцій має базуватися на усталеній моделі інформаційної війни, для кожної сторони конфлікту вона може бути однаковою або різною.[53]

Дооослідження українського вченого Г. Г. Почепцова та деяких інших дослідників, вказують на такі моделі інформаційної війни: модель масової демонстрації; модель пропагандистської комунікації; модель дезінформаційної кампанії; модель кампанії нейтралізації; модель масової комунікації; семіотична модель; модель резонансного впливу[54].

Масова демонстраційна модель. Початок цієї моделі чомусь був покладений у масових заворушеннях громадян, згодом все переросло в бунт, який закінчився поваленням нинішньої влади. Можливо, такий інтенсивний інформаційний вплив вигідний певній групі людей , що призводить до зміни влади.

Яскравим прикладом даної модель виступає Євромайдан 2013 року. Медіа-компонент Євромайдану перебував в центрі уваги з самого початку подій, оскільки нові медіа, особливо соціальні мережі, стали головним рушієм протестного руху. Одне речення Мустафи Найєма у Facebook 21 листопада 2013 року – це маленький початковий крок, який підбурив українське суспільство. Після перших восьми днів Євромайдану можна спостерігати, як інтернет ресурси нарешті почали відігравати значну роль у політичному житті країни. Поява Євромайдану пов'язана насамперед із цифровими комунікаціями в соцмережах та інтернет-медіа. У соціальних мережах фундаментом спілкування є те, що люди прислухаються до думки тих, кого вони добре знають, і їм довіряють. Це можуть бути друзі, близькі родичі, колеги, відомі люди. Можна зустріти багато досліджень, які показують, що головним фактором у визначенні політичних уподобань людини є уподобання її друзів/родичів, а не політична реклама чи заяви політиків. Тому, коли Мустафа Найем, Роман Шрайк, Андрій Шевченко, Леся Оробець та сотні інших людей написали, що йдуть на Майдан – пішли тисячі людей бо мають довіру до них.[55]

Модель пропагандистської комунікації. У даній моделі дослідник Л. Войтасик говорить про три головні кроки розвитку:

- переорієнтацію громадської думки через запровадження нової ціннісної шкали;
- економічна дезінформація;
- поширення споживчих моделей кращого життя через ЗМІ, фільми, серіали тощо. [54, с. 57].

Ці кроки розвитку, дають можливість розвиватись пропагандистській комунікації, але не завжди уявлення про розвиток подій відповідає реальності.

Саме такими кроками і рухається російське керівництво, розповсюджуючи пропагандистські прийоми. Найчастіше ці прийоми вони використовують для того, щоб «очистити своє ім'я» в очах російського населення, таким чином фотодокази з українського боку про злочини російських військових на території України вони перетворюють в зручну та потрібну для них інформацію. Так, коли на простори інтернету потрапили фото поранених жінок після бомбардування у перший день війни у місті Чугуєві Харківської області, російськи пропагандисти назвали це «блискавичною грою». Також, «постановою» вони назвали фото обстрілу пологового будинку в Маріуполі. На фото яке облетіло весь інтернет, де поранені жінки втікають з місця обстрілу була блогерка Маріанна Підгурська, російські ЗМІ та громадяни Російської Федерації почали відкрито цькувати в соціальних мережах цю дівчину, нібито вона за кошти знялась у «виставі», а поранення дівчини в наслідок обстрілу називають «гримом».

Також, прикладом даної моделі інформаційної війни виступає, як російські окупанти на території Чернігівської області примусово роздають «гуманітарну допомогу» для картинки пропагандистських ЗМІ. Іноді, щоб отримати необхідні скріншоти, пропагандисти навіть вдаються до злому сайтів українських державних органів, щоб опублікувати свої неправдиві повідомлення. У подіях, де немає фото/відео доказів, пропагандисти відображають це «дзеркальними історіями». За цим методом більшість злочинів російської армії перетворюються на злочини українських військ, варто лише пропагандистам змінити меседж російських збройних сил до збройних сил України.[56]

Модель дезінформаційної кампанії. Найпоширенішим впливом на масову свідомість через дезінформацію є:

- привернення уваги;
- емоційна стимуляція;
- демонстрація того, як вирішити конфліктну ситуацію, дотримуючись порад комунікатора.

Такі пропагандистські повідомлення є дезінформацією, поширенням чуток, щоб збити людей з пантелику та досягти мети.

Під час повномасштабної війни, яка триває з 24 лютого 2022 року Російська Федерація не раз намагалась підірвати свідомість людей на користь російському керівництву. Таким чином, Російська Федерація розгорнула дезінформаційну кампанію про нібито свою перемогу у війні на Україні. Для поширення чуток про свою «перемогу» кремлівська пропаганда залучила не лише своїх псевдоекспертів а й прихильників путінського режиму, колишнього морського піхотинця США Байрана Барлетика. Цей знавець розповідає, як для англомовної спільноти, так і для російської, нібито на території України, українські військові вбивають своїх громадян, щоб підставити Російську Федерацію. Ворог бачить, що немає перспектив у бойових діях, і він іде шляхом інформаційного нападу на український народ. Таким чином, у людей які змучені від війни може скластися хибне уявлення про дії, які відбуваються в реальності. Так, Кремль намагається розповсюджувати новини про нібито «досягнуті цілі спецоперації в Україні», щоб пізніше видати псевдофакти за докази перемоги.[57]

Модель кампанії нейтралізації. Основними функціями цієї моделі є:

- мовчання конфлікту;
- введення нової події;
- відповіді чи спростування.

Ця схема дозволяє громадськості зосередитися на іншому питанні. На цьому етапі добре побудована інформація погано піддається перевірці, тобто група, якій надсилається повідомлення, часто вірить у це.

Яскравим прикладом моделі нейтралізації, виступає Російська Федерація. Країна нейтралізує всю правдиву інформацію, а розповсюджує ту, яка вигідна їм. Попри те, що російське керівництво війну називає «спецопераціею», вони ще доносять своїм громадянам нібито українські «нацистські організації» несуть загрозу для Російської Федерації, так вважають близько 76% росіян. Також 88% росіян впевнені, що на території України є організації, які «сповідують ідеологію нацизму». 78% населення підтримують дії президента Російської Федерації, а 74% схвалюють його рішення напасти на Україну.[58] Дана статистика показує, наскільки

переконливо працюють ЗМІ в Російські Федерації. Більшість населення, вірять своєму президенту, та підтримують його дії в Україні. А щоб, зосередити увагу громадян на чомусь іншому, В. Путін вирішив «повернути» піонерів у свою країну. Комуністична партія Російської Федерації прийняла у піонери 5 тисяч школярів. Церемонія пройшла на Червоній площі у Москві. Так, громада не говорить про війну, а про новий порядок в Росії.

Модель масової комунікації. Звичайна модель комунікації складається з таких елементів: джерело – кодування – повідомлення – декодування – одержувач [75, с 268].Використовуючи дану модель, є можливість втілювати в життя управлінський вплив на свідомість людей та актуалізувати життєво важливі інтереси різних учасників інформаційного простору[59]. Також, масові комунікації впливають не лише на інформаційний простір а й на політичний.

Дезінформувати населення, це є основним аспектом в моделі масової комунікації. За цією модель працюють російські маніпулятори, які хочуть дезінформувати українців, створити недовіру один до одного, та до керівництва держави в цілому.

Найпоширенішими темами російських пропагандистів є: маніпуляція про мобілізацію, заборона перетину кордону чоловікам, відкриття нових напрямків бойових дій, гуманітарна допомога та провокація. У телеграм-каналах та вайбер-чатах неодноразово можна було зустріти повідомлення про ізраїльську розвідку, яка повідомляє, що Російська Федерація нарощує військовий контингент у Бресті. Також не раз, можна було почути та побачити інформацію нібито про те, що працівники військкомату мають на меті відправити більшу кількість чоловіків із Західної України, і також засудження чоловіків-біженців з інших областей України, які нібито не хочуть захищати свої домівки.[60]

Отже, даною метою окупантів виступає створення напруженості в суспільстві, негативні реакції та емоції. Тому, вони використовують чутливі теми, які впливають на підсвідомість людей, та залякують їх.

Семіотична модель. Дослідник Ч. Пірс, виділяє три типи семіотики[54, с. 210]:

−іконічні знаки у вигляді телевізійних;

−знаки, що вказують на іншу реальність, яку вони представляють;

−знаки-символи, тут ключову роль відіграють ЗМІ, які вносять нові пріоритети для суспільства та змінюють їх ієрархічний статус.

Зміна цих кодів змінює державу, держави також можуть зникнути, прийнявши чужі коди.

Так, російські керівники та й російські окупанти використовують ідеологію знаку «V» та «Z», саме ці букви означали приналежність техніки до того чи іншого виду військ, або ж до якого військового округу належать частина – так вважали наші воєнні та громадяни. Але як виявилось «Z» – це за перемогу , а «V» – сила в правді, а трикутник «Завдання буде виконано». Цю ідею підтримали багато чиновників Російської Федерації. Ця ідеологія дійшла до того рівня, що на всіх вивісках, оголошеннях, офіційних звернень були присутні ці знаки. Дітей в російських школах змушують виступати з цими знаками, проводяться різні флешмоби де ж знову таки головним атрибутом є ці букви. Також на окупованих територіях, ці знаки можна зустріти всюди, особливо на будинках які були розгромлені або на машинах і т.ін.

Підтримуючи цей метод пропаганди, російське керівництво прагне пробудити в людей патріотизм, вірність і позитивне ставлення цієї «воєнної операції». Саме тому, вони пофарбували символи у кольори георгіївської стрічки, щоб якимось чином пов’язати це з Другою світовою війною і так виправдати всі свої дії. Весь цей абсурд, нагадує лише одне – свастика Гітлера. І це лише в який раз доказує нам, що російські окупанти та сам головнокомандувач Російської Федерації вчиняють так як нацисти.[61]

Модель резонансного впливу. Резонансну модель можна розглядати як ситуацію, в якій вхідна інформація набагато менша за вихідну. Використання резонансних технологій можна уявити як айсберг. Масова свідомість зосереджена на вершині айсберга, який спрямовує всю відповідну інформацію. Стимулюючи дискусію, завданням має бути вибір таких ключових повідомлень, які стимулюють обговорення ситуації в певних цільових групах населення. На виході соціального підсилювача виникає потужний сигнал. Результатом стають акти насильства, які індивіди у відриві від групи, можливо, ніколи б не вчинили.

Багатоканальний вплив, коли аудиторія отримує повідомлення одного типу через кілька каналів. Перевагами такого підходу є:

- менше суперечливих повідомлень починає циркулювати в середовищі;
- одне й те саме повідомлення буде чути з різних джерел;
- характеристики кожного каналу можна максимізувати.[53]

Прикладом резонансної моделі, виступають дії, які відбувались в Гостомелі, Бучі, Ірпені, Ворзелі, Бородянці на Київщині. Саме ці міста з перших днів російського вторгнення стали епіцентром бойових дій. Головною причиною ситуації, у якій опинилися Буча та Ірпінь, став напад з території Білорусі. Саме з її території на північ Київської області у перший день вторгнення, 24 лютого 2022 року, почали заходити російські війська, метою яких була українська столиця.

3 квітня 2022 року Київська область була звільнена від російських загарбників. Радість визволення перервали жахливі кадри з вулиць Ірпеня, Бучі та Гостомеля. Російські окупанти залишили після себе розграбовані будинки, повні руйнування і сотні вбитих мирних жителів, тіла яких просто заполонили вулиці зруйнованих міст. Деякі люди були закуті наручники, а значить, катували людей, по кадрам які були розміщені на просторах інтернету були помітні вистрілили в потилицю та зґвалтування. Шокуюче те, що в Бучі виявили братську могилу, в якій було майже 300 осіб. Ці міста є картиною постапокаліптичного фільму жахів. Серед жертв цих військових злочинів, які вже виявили російські війська, є зґвалтовані жінки, яких намагалися спалити, вбивали місцевих чиновників, вбивали дітей, вбивали літніх людей та вбивали чоловіків. Перелік тортур, які робили російськи окупанти можна перелічувати ще довго, але головна суть цього є що це був справжній геноцид українського населення. [62]

Порівнюючи моделі інформаційної війни, можна дійти висновку, що всі моделі пов’язані між собою, вони мають спільну ціль, але не завжди один й той самий об’єкт. Хоч і мета моделей однакова, але результат завжди різний. Дивлячись, як ворог веде інформаційну війну та на які моделі він опирається, так можна і передбачити можливий розвиток подій та змусити противника змінити модель поведінки завдяки явних і прихованих, зовнішніх та внутрішніх інформаційних загроз.

Прихована загроза – це ненавмисне проникнення в систему в режимі реального часу, що загрожує її безпеці. Чи є можливість передбачити поведінку противника і з якою точністю. Відповідь на це питання визначається в кожному конкретному випадку конкретним результатом інформаційного моделювання поведінки конкретної системи.

Аналізуючи моделі інформаційної війни та особливості їх впливу на підсвідомість населення, дає можливість зрозуміти, що такий вплив може нести в собі не лише дрібні заворушення а й значні мітинги, які несуть за собою вплив на політичну діяльність країни.

Виходячи з наведених вище прикладів та порівнянь, можна стверджувати, що трансформація моделей інформаційної війни, так як у війні Росії з Україною. Те, що показали ЗМІ, не мало реального підтвердження – це і є модель віртуалізації. Ця пропаганда була започаткована на емоційному контексті, тому в неї було легко повірити. Раніше ця модель не використовувалася в інформаційних війнах. Досвід цієї війни дав чітко зрозуміти, що в сучасному світі інформаційна зброя не менш загрозлива, ніж військова.

Сучасна інформаційна війна – це стратегія цілеспрямованих дій для досягнення цілей, але зараз в Україні немає розуміння необхідності її використання як способу протидії експансіоністській діяльності країни-агресора.[63]

3.2. «Фейк» як інструмент інформаційної війни

Досліджуючи класичну працю давньокитайського стратега Сунь Цзи «Мистецтво війни», бачимо, що сутністю будь-якої війни є обман. Саме так, більшість громадян проти яких ведеться інформаційна війна не до кінця розуміють всю суть проблеми та всієї загрози, яка їх чекає, оскільки вони затьмарені великою кількістю неправдивих меседжів.

Чим більше почало розвиватись інформаційне суспільство, тим більше і розповсюджується неправдива інформація, свій початок «фейки» беруть ще з

традиційних ЗМІ. Але все ж таки, друковані видання не цілком придатні для розповсюдження підробок.

Традиційні видання, не є таким ефективним представником розповсюдження інформації як електронні ЗМІ, тому що наступний номер видання вийде не раніше ніж завтра, а в інтернет-просторі фейкові новини розлітаються миттю. Також, друковане видання є документом, і таким чином автор або видання можуть нести відповідальність за розповсюдження неправдивої інформації. Радіо теж не підходить для поширення недостовірної інформації через свою фонову природу.

Фейкові новини – підробка чи імітація новин (маніпулятивне спотворення фактів; дезінформація). Для створення фейків використовують змінені або вигадані історії, божевільні теорії змови, містифікації, сфабриковані фото та відео. Фейкові новини розлітаються у шість разів швидше за правду. Це потужний інструмент, з яким можна вплинути на думку людей і переконати їх в будь-якому факті.

Цікаво описує методи спеціальної бойової пропаганди журналіст В. Яковлєв. Аналізуючи його статтю, можна сказати, що в обставинах секретності студенти вчили бойові спецпропаганди – вміння сіяти розлад на території ворога завдяки розповсюдження фейків та маніпулювання свідомістю населен Метод «гнилого оселедця», метод «перевернутої піраміди», метод «великої брехні», метод «40 на 60», метод «абсолютної очевидності» - всі ці методи і прийоми є спільними для всіх користувачів Інтернету, але вони просто не усвідомлював цього. Майбутніх журналістів навчили використовувати спеціальні методи пропаганди проти ворожих солдатів.

Якщо розглянути метод «гнилого оселедця» то він працює за такою схемою: вибирається неправдиве звинувачення, це бувають дрібні крадіжки, вбивство, жорстка поведінка з дітьми. Мета цього методу не в тому, щоб довести хто винний, а хто ні, а в тому, щоб направити громадські обговорення навколо цієї теми. Наша психіка сформована так, що як тільки звинувачення стають все більш глобальними, то завжди знайдуться прихильники чи противники, експерти чи опоненти. І таким чином, не зважаючи на свої погляди, усі учасники обговорення неодноразово вимовили ім’я обвинуваченого.

Метод 40 на 60 винайшов Геббельс. Він полягає у створенні ЗМІ, які надають 60% інформації в інтересах ворога. Завоювавши таким чином його довіру, решта 40% використовують це як надзвичайно ефективну, завдяки цій довірі, дезінформацію.

Всі методи боротьби з фейковими новинами об'єднані однією метою. Це послаблення ворожої армії шляхом насадження в її лави внутрішньої ворожнечі, взаємної ненависті та недовіри один до одного. Сьогодні ці методи використовуються проти нас. Результат, до якого вони призводять, це те, для чого вони створені. Проте взаємна ненависть і внутрішня ворожнеча виникають не у ворожій армії, а в наших домівках і родинах.[64]

Тепер усе може бути фейком, відредаговані фотографії, штучно змонтоване відео, написані чи сфабриковані фейкові новини, які важко відрізнити від правди. Підробкою вважаються також фейкові акаунти неіснуючих людей у соціальних мережах, через які поширюється недостовірна інформація.

Головною метою неправдивих повідомлень як інструменту інформаційної війни – це викликати у людей сумніви, переконати аудиторію в достовірності наданої інформації. Завдання – дезінформувати аудиторію, просувати власне бачення, політики чи позиції, викликати агресію; похитнути позицію особистості і змусити її засумніватися; поширення паніки; редагування мислення аудиторії; провокування певної дії; підвищення уваги та інтересу аудиторії; заспокоєння аудиторії за допомогою вигаданих фактів; залякування аудиторії тощо.[65]

Більшість фейків має панічний характер. У фейках в більшості є прохання за термінове поширення або заклик оприлюднити цю інформацію у своїх соцмережах. Дуже часто в підробках немає посилання на джерело. Також джерелом можуть бути невказані, скажімо, чиїсь родичі в адміністрації чи правоохоронних органах. Кожна інформація має вагу і значення. Тому його слід публікувати на сайтах, які також мають вагу – на сторінках влади, авторитетних ЗМІ.

Головна мета – посіяти паніку, деморалізувати українське суспільство. Змусити повірити, що ми програємо війну. Сам тому у воєнний період важливо мати тверезу голову, критичне мислення, і все-все, що ви бачите, піддавати сумніву.

Основні ознаки фейку:

- Простота та ясність. Фейки не виникають нізвідки. Вони з'являються там, де є шум та інформаційний вакуум. Коли є актуальна проблема, про яку мало відомо, люди починають задавати питання. Якщо влада та експерти не реагують, починають поширюватися найпростіші та зрозумілі підробки. Тому щоразу, коли пропонується проста відповідь на складне питання, є привід засумніватися.
- Емоційність. Розрізняють два типи мислення: раціональне та емоційне. Коли ми мислимо раціонально, ми не віримо в дурниці. Однак коли хтось починає маніпулювати важливими для нас темами, всяка раціональність відходить на другий план. Наприклад, коли ЗМІ пишуть щось про здоров'я чи дітей. Ми хочемо захистити себе та своїх близьких від неприємностей, тому віримо емоційним новинам і розповідаємо про них іншим.
- Відсутність посилань на джерела або на офіційні канали комунікації.[66]

З початком українсько-російської війни, українці не раз зустрічались з фейковими новинами. Такими методами, російська влада намагається дезорієнтувати українську громаду. З кожним роком зростання фейків все більше і більше, причиною тому слугує великий вплив інформаційного простору на сучасне населення.

Інформаційна пропаганда Москви поширюється в популярних українських соціальних мережах Facebook і Twitter, намагаючись маніпулювати поглядами потенційних виборців шляхом поширення дезінформації, чуток і брехні. Люди рідше звертають увагу на повідомлення, які не відповідають їхнім переконанням. Але неправдива інформація підступно структурована таким чином, що порушує захисний кодекс нетерпимості, створюючи сумніви там, де все здавалося таким очевидним. В Україні слово фейк лунає на телеекранах, у медіатекстах.

Кремлівські пропагандисти ефективно користуються маніпуляцією людей та залякування їх, шляхом розміщення в усіх можливих пабліках, групах, спільнотах інформація яка не є достовірною, яка зачіпає кожного громадянина. В соцмережах, окупанти розміщують навчальний матеріал як правильно розповсюджувати фейкові новини, як впливати на їхню свідомість, з певними прийомами, спираючись на знання «української психології». Російські пропагандисти виділяють чотири основні пункти у створені фейків:

– Інформація повинна бути простою, банальною. Щоб вплинути на всі верства населення, не потрібно придумувати нічого надприродного. Можна добавити трохи абсурду.

– Фейк повинен нести за собою сильний меседж і залишити місце для власних фантазій.

– Пропаганда має спиратись на місцеві особливості. Достовірності йому надає точне знання географічного положення певної місцевості.

– Чим більше людей розмістить цю «інформацію», тим більше буде позитивних результатів. [67]

Щоб чіткіше зрозуміти термін «фейк» проаналізуємо, які саме фейкові новини розповсюджуються по Україні і як вони впливають на українську спільноту.

Російська влада ганебно уникає слова «війна», за його вживання можна отримати справжнє тюремне ув'язнення. Тому в Росії смертельний напад на Україну називають «спецопераційою». Але очевидно, що коли армія вторгається в іншу країну, обстрілює міста, вбиває мирне населення, руйнує інфраструктуру, бомбить дитсадки, пологові будинки та лікарні, це війна і тероризм.

Білоруське видання «Белновости» розміщує фейкову інформацію про те, що нібито після обстрілу АЕС у Запоріжжі, був нанесений удар окупантами по Рівненській атомній станції в місті Вараші. У даному матеріалі, білоруси запевняють, що російські війська мають на меті знищити все, і путінська армія веде війну по самознищенню, тому що ядерна хвиля накриє не лише територію України а й Росії, і що це спровокує початок ядерної війни для всієї Європи.

Також відомо, що російські окупанти організовують у Херсоні мітинги для «картинки». Вони в пошуках нових методах дезінформувати українців та виправдати свої агресивні дії принаймні перед власним народом. Таким чином, до Херсона привозять кримчан для участі у мітингу. Відомо, що окупанти заволоділи складом з одягом водної поліції, тож на мітингу були присутні переодягнені російські військовослужбовці, які у вигляді українських поліцейських «дякують» окупантам. Подібні дії окупанти організовують для своїх ЗМІ. В таку картину можуть повірити лише росіяни, які досі вірять, що їхня армія проводить «спецоперацію на Донбасі».

Російські пропагандистські сайти поширюють фейк про те, що українські військові свідомо не відпускали мирних жителів Маріуполя. Зокрема, фейки публікували sm.news, Перший канал, Аргументи тижня, Взгляд, Московський комсомолець, ТАСС та інші. Насправді місто було заблоковано російськими окупантами, обстрілюючи критичну інфраструктуру та не допускаючи продовольства.[68]

Від початку війни Росії проти України інформаційний простір став полем запеклої боротьби між окупантами та українським народом. Але підробки часто поширюють не лише російські окупанти. У величезному інформаційному потоці цим свідомо користуються грабіжники і часто несвідомо звичайні українці.

Російські творці фейків, розуміють що інформація, яка несе за собою доказ фотографіями, аудіо записом, відео сприймається з більшою довірою. Але в більшості коментарі чи підводки до цих доказів надають нам готове пояснення, зосереджуючи на повне сприйняття того, що ми бачимо.

Величезна кількість російських спеціалістів працює над інформаційно-психологічними операціями проти України. У міру просування військових на землі та в повітрі атака в інформаційному просторі має декілька завдань:

- Дезорієнтувати військових. Вони витрачають ресурси у відповідь на повідомлення про загрози, яких насправді не існує.

- Деморалізувати військових. Для цього їм всіляко кажуть, що чинити опір немає сенсу, керівництво держави втекло і всіх здало, що нібито військовослужбовці вже склали зброю і радять їм це зробити якнайшвидше. Професійні солдати зазвичай вчаться протистояти такому впливу, але цивільні особи, які вступили в армію, можуть постраждати.

- Деморалізувати мирних жителів. Налякати, паралізувати всіх страхом за своє життя та життя своїх дітей. Агресор сподівається, що суспільство налякається і попросить керівництво держави припинити військові дії за будь-яких умов.

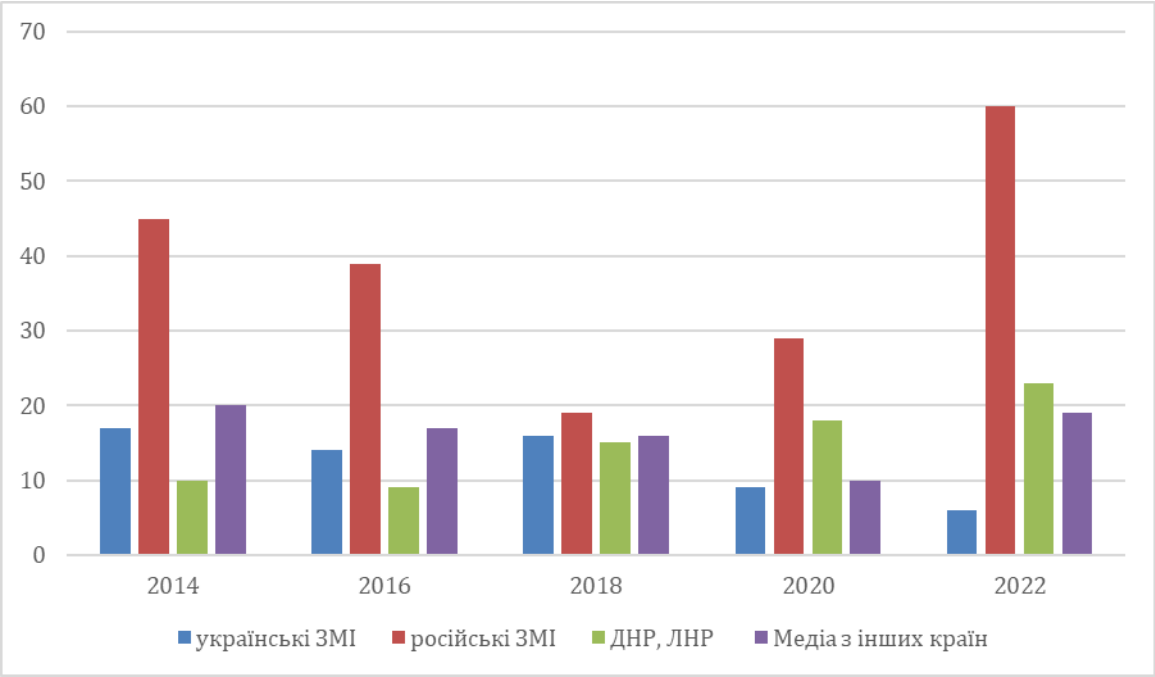
- Паніка. Військовим набагато складніше захищатися, коли дороги перекриті біженцями. Цивільній владі важче забезпечити тих, хто цього потребує, і утримати

економіку від колапсу, коли натовпи штурмують банкомати та викрадають все з магазинів.

− Створіть колапс в інформаційному просторі. Для цього за допомогою соціальних мереж, месенджерів, підконтрольних агресору видань у ЗМІ насичують інформаційний простір величезною кількістю фейкових повідомлень. Деякі з них здаються правдою, інші ні; в деяких є частка правди, деякі можуть бути виділені як абсурдні. Здатність людського мозку споживати й аналізувати інформацію обмежена, тому людина, занурена в отруєний інформаційний простір, незабаром впадає в ступор. Вона більше не бачить межі між реальністю і вигадкою. Вона може почати вірити будь-якому неправдивому повідомлення або, навпаки, побачити підробки в повідомленнях офіційних джерел.[69]

Найбільша увага російських пропагандистів зосереджена на діях, що відбуваються в Маріуполі та на полк «Азов» в цілому. Окупанти запевняли, що полк користується житловими будинками як прикриттям, і стріляє по мирних жителів. Також, часто можна зустріти повідомлення, що нібито російська армія рятує дітей з Маріуполя, батьків яких розстріляли «українські нацисти». По місту їздили машини і на гучномовці говорили, що Запоріжжя вже не приймає переселенців, щоб вони всі виїжджали в Росію, в безпечне місце. Що, нібито Одеса під російським керівництвом. Ці дії, вони робили для того щоб збити з пантелику населення міста, та породити недовіру до влади.

Отже, аналізуючи всі фейки, які були розміщені протягом 2014-2022 років, вивівши всю статистику а діаграму, чітко видно що в 2014 та 2022 рік найбільше розповсюджувалось фейків. У період з 24 лютого по 2 квітня 2022 року в середньому вдень випускалось 2-3 фейкових новини. На діаграмі ми бачимо, що найбільшим пропагандистом являється російське ЗМІ.



Загалом можна зробити висновок, що нині демократичне суспільство змушене балансувати між двома крайнощами. З одного боку, без свободи слова не буває демократії, а з іншого – існує загроза використання свободи слова для маніпулювання масовою свідомістю. Для розробки ефективних механізмів протидії важливо проаналізувати потреби громадян, яку інформацію вони обирають, з яких джерел, критерії достовірності, як вона впливає на свідомість, емоційне вираження, як громадяни ставляться до ЗМІ, державних установ тощо.

Щоб протистояти хитро використаній дезінформації та маніпуляціям, насамперед російськими ЗМІ, які поширюються через соціальні мережі та інші канали комунікації, кожній країні потрібна консолідація, довіра до влади та масштабна інформаційна політика для швидкого реагування. сучасні технології. При цьому громадяни повинні правильно фільтрувати інформацію, критично мислити, аналізувати, звертати увагу на джерела інформації, власників ЗМІ, адже з підвищенням обізнаності маніпуляції зменшуються.

3.3 Методи боротьби та протидії інформаційної війни між Росією та Україною

Протидія інформаційній війні є одним з головних напрямків для забезпечення інформаційної безпеки держави.

Щоб ефективно боротися з впливами інформаційної війни, потрібно вживати регулярних контрзаходів протидії. Важлива роль у вирішенні цієї проблеми відводиться ЗМІ. Факти, які розміщуються в ЗМІ, зосередження на певних явищах чи аспектах протистояння, створюють громадську думку про війну, зосереджуючи правильну реакцію. ЗМІ мають змогу перетворити маленький конфлікт у велике протистояння або, навпаки, швидко вирішити глобальну проблему. Перебіг самого конфлікту багато в чому залежить від ставлення ЗМІ до події, їх упередженості та прихильності. Вагому роль у боротьбі з інформаційною війною відіграє суспільство, люди з активною життєвою позицією, які передають в Інтернет інформацію, відмінну від нав'язаної суспільству ззовні.

Вигідними рекомендаціями протидії інформаційній війні, також можна вважати виготовленні для бізнесу повчання з протидії в інформаційному просторі, що можуть бути пристосовані до більш масштабного використання. Підвищити у населенні аналітичні спроможності, навчити методам критичного аналізу меседжів, зберегти від інформаційних диверсій – це один з найскладніших та найдовших методів протидії інформаційній війні, але вважається одним з дієвих способів.

Щоб протидіяти інформаційній війні, потрібно ввести підсистему активних дій з інформаційного впливу. Здійснення цієї підсистеми потрібно систематизувати у межах політики інформаційного протистояння, використовуючи можливості Служби безпеки України. Зі створення потрібного центру протидії та його роботи, дане питання краще розглядати з точки зору можливостей організації на громадських засадах за рахунок донорських вливань. Це б дозволило будувати більш еластичну та мобільно сучасну структуру інформаційного протистояння.

Для більш позитивних результатів діяння центру, він повинен співпрацювати з державними органами країни. Аналізуючи інформаційну війну Росії з Україною, головними функціями у роботі даного центра повинні бути:

- Зосередження діяльності волонтерів щодо моніторингу медіа-ресурсів на предмет наявності матеріалів, які згубно впливають на інформацію, а також здійснення такої діяльності працівниками організації. Наприклад, слідкувати за матеріалами, які можуть нести загрозу громадянам країни або ж самій владі країни. Відслідковуючи таку інформацію, повідомити правоохоронні органи в разі небезпеки.
- Заохочувати населення до створення ресурсів для виявлення неправдивих інформаційних повідомлень, а також для представлення результатів у загальнодоступній формі.
- Створення певних порад до чинного законодавства органам законодавчої та виконавчої влади на рахунок вдосконалення системи інформаційної безпеки країни.
- Доведення до народу країни, яка має деструктивну дію інформації, достовірної інформації та формування умов для критичного аналізу громадянами цієї країни інформації з відповідних ЗМІ.
- Адаптація сучасних методів інформаційного протистояння до внутрішніх реалій та надання рекомендацій щодо їх застосування відповідними державними органами.[70]

Для більш точного формування методів та протидій інформаційній війні між Росією та Україною, слід сформулювати SWOT-аналіз.

Сильні сторони	Можливості
Підвищення ефективності політики інформаційної безпеки в галузі оборони	Формування та здійснення взаємовигідного зв’язку між Україною та міжнародними альянсами
Духовна й політична єдність української спільноти	Вирішення суперечностей між сучасними центрами сили щодо

	оцінки та врегулювання інформаційної безпеки України
Вдосконалення методів безпеки інформаційних і телекомунікаційних систем, а також систем та засобів інформатизації озброєння і військової техніки, систем управління військами і зброєю.	Більше зосередження влади в сфері розвитку інформаційного протиборства
Підготовка у навчальних закладах у сфері протистояння інформаційним війнам	Активізація процесів світової співпраці у різних формах
Слабкі сторони	Загрози
Не контрольованість виникнення нових електронних ресурсів та інформаційних площин	Відсутність взаємовигідного діалогу між Україною та міжнародними організаціями
Психологічне маніпулювання населення неправдивою інформацією	Загострення суперечностей між сучасними центрами сили щодо оцінки та врегулювання інформаційної безпеки України
Вільне проникнення в супутникові ЗМІ, соціальні мережі, та електронну пошту пропагандистських матеріалів	Політична незацікавленість в розвитку інформаційного протиборства
Поверхневе навчання фахівців з інформаційної безпеки та кіберзахисту	Пряма збройна агресія

Сучасна інформаційна війна Росії проти України, дала можливість чітко зрозуміти, що пропаганда є основною інформаційною зброєю, що захоплює людську підсвідомість, забираючи можливість свідомо мислити та приймати зважені рішення. Для зрушення стабільної системи інформаційного простору Російська Федерація

використовує всі можливі канали для розміщення дезінформації: телебачення, Інтернет, преса, радіо, чутки, експертне середовище. Щоб чіткіше сформулювати всі можливі протидії цій кампанії, слід визнати її сильні сторони. До головних переваг даної кампанії можна віднести: всеосяжність та системності задуму, зосереджена центральна виконавча вертикаль, притягнення великих матеріальних та громадських ресурсів, значний рівень медіапростору, високий технічний рівень, високі вміння маніпулювання людьми та гра на почуттях. Виходячи з цих сильних сторін, можна сформулювати основні задачі протидії:

- Правоохоронна операція щодо забезпечення демократичних засад держави. Це контррозвідувальна, оперативно-розшукова та процесуальна робота, спрямована на фіксацію та знищення системи поширення різноманітних звернень. В умовах ескалації загроз особливо важливу роль відіграє РНБО як орган, що координує діяльність правоохоронного та безпечного сектору держави та підконтрольний главі держави. Саме цей орган має всі необхідні організаційні фактори для об'єднання різноманітних органів (прокуратури, Служби безпеки, МВС, фіскальних органів) для протидії єдиній ворожій пропагандистській системі.
- Робота зі змістом, тобто зі змістом інформації, що створює бачення світу для людини. Вважається запровадження стимулів до створення особистого інформаційного продукту, виготовленого на власному історичному досвіді з урахуванням власних цілей та особливостей.
- Постійний розвиток власного інформаційного простору. Зняти з українського інформаційного середовища глобальну залежність від російського інфо-простору, тобто виведення України з-під юрисдикції московських офісів Google, Facebook та інших.
- Реалізація «стратегічних комунікацій» системи управління. Насправді це зосередження обов’язків влади інформувати громадськість. Значні комунікації дають зрозумілу мету та постійне розміщення інформації про те, як ми досягаємо наших цілей.

Якщо аналізувати вище сказане, слід зазначити як повинні базуватись протидії інформаційній війні в умовах війни Росії з Україною:

− Доречно організовувати протидію інформаційній агресії Росії за допомогою інструментів Ради національної безпеки і оборони під єдиним керівництвом глави держави.

− Система повинна включати як заходи боротьби з незаконною діяльністю, так і заходи щодо заохочення розвитку відповідних місцевих виробництв. Протидія працює шляхом притягнення до відповідальності та регулюючих заходів, стимулювання розвитку - через економічні та організаційні дії.

− Вся система має бути охоплена єдиним планом, керована та пов'язана з населенням через мережу стратегічних комунікацій.

− Присутня потреба для більш ширшого прийняття меж теорій кримінального права комплексних обставин, дій, доказів, що сформовують об’єктивну сторону складу, широко розповсюдженого злочину, такого як пропаганда. А задля цього потрібно розширити правове поле, в рамках якого глобально буде визначатись такі поняття, як « російська пропаганда», «пропаганда війни», «протидія російській агресії» тощо. Тобто, більш широко дивитись на елементи ведення інформаційної війни, сприйняття гібридної війни як частину окремих проявів кримінально-караного діяння.

Зрозуміло, що головною проблемою є вузькі можливості застосування до цих дій категорії «пропаганда війни», зміст інформаційних посилань, які Російська Федерація використовує через російські ЗМІ та соціальні мережі. Визначити безпосередню шкоду, заподіяну такими діями, важко, а отже і ідентифікувати потерпілого майже неможливо, але якщо не враховувати шкоду та зосередитися на характері дії – незаконне втручання у внутрішні справи Української держави з метою дестабілізації ситуації, створення негативного іміджу, дезінформації, пропаганди чи будь- якої форми ворожості – все це слід розуміти як пропаганду війни з боку Росії.

У певному сенсі це можна вважати політичним рішенням, але йдеться про протидію російській агресії як комплексу заходів і механізмів протидії інформаційній війні. Поняття інформаційної безпеки за своїм негативним впливом та значущістю для українського суспільства ототожнює інформацію, яка сприяє прояви війни, до ще

інших видів інформації, яка будь-яким чином розпалює ворожнечу, підриває територіальну цілісність чи державний суверенітет тощо. [71]

Якщо враховувати високий рівень небезпеки, що несе за собою діяльність суб'єктів інформаційних війн державним підрозділам та міжнародним організаціям, рекомендується запровадити низку нормативно-правових актів, які включають в себе всі можливі сучасні інформаційні технології у напрямку державного управління, збільшити спроможність державних органів влади і місцевого правління до використання певних дієвих технологій управління.

На сьогоднішній день, інформаційний простів України не до кінця під захистом від нападів інформаційних впливів, загроз, фейків і тд. Тому, для повного забезпечення країни, створення дієвої системи інформаційної безпеки в Україні, активізування ефективних стратегій і протидій ризику нападу на інформаційний простір, повинні бути на першому місці для органів державної влади та глави держави.[72]

Для протидії масштабним інформаційним впливам з боку Росії, розроблені такі кроки:

- зливання України з міжнародним та європейським інформаційним простором
- вхід України у глобальні, міжнародні інформаційні організації
- формування особистої інформаційної моделі та забезпечення розвитку інформаційного суспільства
- покращення системи безпеки інформаційного простору країни та поліпшення інформаційної політики
- розвиток національної інформаційної інфраструктури[73]

Отже, підсумовуючи вищесказане, можна дійти висновку, що боротьба з інформаційною війною є одним із напрямів забезпечення інформаційної безпеки як частини національної безпеки.

Механізми протидії цим загрозам мають бути високотехнологічними та систематичними. Для позитивного результату необхідно не декларувати, а розпочати створення системи безпеки інформаційного простору, а також забезпечити

функціонування центру реагування та спеціальних операцій з нейтралізації інформаційних загроз.

Доречно ввести в навчальний процес, починаючи зі старших класів школи, хоча б факультативні заняття з «Основ інформаційної безпеки». Це дозволить стратегічно підійти до вирішення даної проблеми.

Підтримка держави в ініціації та проведенні досліджень проблем інформаційного протистояння та розвитку механізмів захисту. Для цього слід залучати фахівців з багатьох галузей знань: медичних, технічних, психологічних, юридичних тощо.

На міжнародному рівні необхідно активізувати дискусію щодо врегулювання в рамках ООН та інших міжнародних організацій безпеки визначення та заборони інформаційної агресії та інформаційної зброї. Ці заходи далеко не вичерпні, але їх необхідно вжити одночасно якомога швидше.

ВИСНОВКИ

Досвід воєн і конфліктів у світовій історії показав, що кожна нова сфера людської діяльності стає сферою збройної боротьби, такою зброєю сьогодні стала інформація, яка передує формуванню інформаційних війн у суспільстві.

Загалом світ не стоїть на місці, технічний прогрес озброює сучасну людину не тільки новими, вдосконаленими засобами виробництва і зв'язку, а й засобами знищення себе та інших. Сьогодні людство досягло такого прогресу, що стало неможливим контролювати деякі глобальні природні явища, екологічна зброя може штучно створювати урагани, шторми, цунамі. На такій війні гине багато людей, і якщо кожен з нас не замислюється про таку проблему, то найближчим часом можна просто знищити себе.

У ході дослідження ми визначили основні положення українського законодавства щодо ведення інформаційної війни. Також ми виявили, що інформаційна війна є багатогранним і досить складним явищем, яке має місце в різних вимірах. Розглянули форми, види та методи ведення інформаційної війни. Крім того, ми змогли дослідили інформаційну війну між Росією та Україною в період 2014-2022 роках. Визначили загрози «фейку» як інструменту інформаційної війни в нашій країні. Також, ми розробили методичні рекомендації щодо протидії інформаційної війни.

Підсумовуючи вищесказане, можна зробити наступні висновки.

Інформаційна війна як складова збройного конфлікту не є новим явищем, але сучасні інформаційні канали ще не захищені від зовнішніх впливів і через брак ресурсів часто стають найвпливовішою зброєю в руках пропагандистів.

Оскільки інформаційна війна взаємодіє з методами психологічної маніпуляції для задоволення власних інтересів і досягнення конкретних цілей, її можна вважати глобальним явищем, що безпосередньо впливає не тільки на хід і результати бойових дій, а й на їх сприйняття та інтерпретацію.

У цій роботі ми проаналізували репортажі російських телеканалів, виявили в них низку ознак інформаційної атаки на Україну – перетягування, спотворення,

поширення чуток та шахрайства. З огляду на те, що багато громадян України є споживачами ЗМІ в Російській Федерації, вони є потенційними жертвами інформаційної війни. На жаль, сучасний український інформаційний простір демонструє незахищеність від зовнішнього впливу військової пропаганди. Україна повинна на законодавчому рівні врегулювати питання інформаційної війни.

Попри це все, з перших днів вторгнення Російської Федерації в Україну багато ІТ-спеціалістів долучилися до спротиву агресору: стали до лав ЗСУ та ТРО або протидіють ворогу на інформаційному фронті. Зокрема спростовують дезінформацію, фіксують воєнні злочини та допомагають військовим та населенню шляхом створення корисних чат-ботів.

Одним із перших на інформаційному фронті з'явився чат-бот загальнонаціональної системи гуманітарної допомоги «Республіканський (Громадянський) штаб солідарності». Над його створенням працювали спеціалісти цілої низки громадських об'єднань, спільнот, профспілок та органів студентського самоврядування за підтримки МОН України та місцевих органів влади. Shelter — наступний чат-бот на базі конструктора SendPulse. Він надає вимушеним переселенцям інформацію про пункти прихистку в Івано-Франківській, Львівській, Чернівецькій та Вінницькій областях. Цього помічника на прохання Асоціації сільських, селищних рад та об'єднаних громад України розробив Олександр Кирієнко, менеджер із внутрішніх комунікацій «Укрзалізниці». Таких чат-ботів з кожним днем стає все більше і більше, це ще один метод протидії війни України з Російською Федерацією.

Також, з початку повномасштабного вторгнення найбільші мовники («1+1», «UA: Перший», «Рада», «ICTV», «СТБ» та «Україна 24») об'єдналися у спільний телемарафон «Єдині новини», щоб озвучувати офіційну позицію держави. Крім того, в нас діє велика мережа організацій, які борються з дезінформацією, на кшталт «Детектор медіа», StopFake, VoxCheck. Всі вони аналізують роботу ворога в інформаційному полі та виробляють текстовий, аудіо- та відеоконтент різними мовами. Держава створила Центр протидії дезінформації при РНБО та Центр

стратегічних комунікацій та інформації безпеки при Мінкультури та інформполітики, які докладають зусиль до боротьби в інформаційному просторі.

Отже, в умовах сучасних інформаційних протистоянь, національний інформаційний простір України є захищеним але недостатньо від негативних пропагандистських інформаційно-психологічних впливів, загроз. Тому створення потужної та ефективної системи інформаційної безпеки України, розроблення дієвих стратегій і тактик протидії загрозам повинні стати пріоритетними завданнями органів державної влади та недержавних інститутів.

СПИСОК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Павлютенкова М. Ю. Інформаційна війна: реальна загроза чи сучасний міф? Влада: 2001. № 12. С. 19-23.

2. Зіма І.І., Ніколаєв І.М. Інформаційна війна та інформаційна безпека(огляд думок зарубіжних політологів та воєних спеціалістів) // Наука і оборона – 1998. – № 1. – С. 56-58

3.Леонтьева Л. Є. Пропаганда як інформаційно-психологічний складник політичних процесів: Монографія. Львів. нац. ун-т ім. І. Франка. Київ; Львів: «ФАКТ», 2004. 298 с

4.Поняття інформаційно війни: веб-сайт. URL:http://politics.ellib.org.ua/pages-8282.html (дата звернення: 06.04.2022)

5.Манойло А. В. Державна інформаційна політика у особливих умовах. М., 2013. 388 с

6. Чорноус, І.С. Інформаційна війна як засіб конкурентної боротьби фахівців з паблік рилейшнз веб-сайт. URL: http://www.rusnauka.com/2_KAND_2014/ Economics/6_153509.doc.htm (дата звернення: 21.05.2022)

7. Маніпуляція свідомістю у ЗМІ і не лише: веб-сайт. URL: http://rusrand.ru/analytics/manipuljatsija-soznaniem-v-smi-i-ne-tolko (дата звернення: 16.04.2022).

8. Дмитро Кулеба. Війна за реальність. Як перемагати у світі фейків, правд і спільнот.— Київ: Книголав, 2019. — 384 с.

9. Інформаційна боротьба у воєнних конфліктах другої половини XX століття. Монографія. – К.:Альтерпрес, 2006. – 192 с.

10. Черешкин Д.С., Смолян Г.Л., Цыгичко В.Н .Реалии информационной войны// Конфидент. 1996. №4. С.9-12.

11. Бутранец В. К. Информационное противоборство: понятие, субъекты, цели / В. К. Бутранец. // Государственное управление и право. – 2008. – № 3 (28). – С. 104-109

12. Манойло А. В. Государственная информационная политика в особых условиях : монография / А. В. Манойло. – М. : МИФИ, 2003. – 388 с.

13. Завдання, об'єкти посягань та форми проведення інформаційних війн: веб-сайт. URL:https://pidru4niki.com/16090322/politologiya/zavdannya_obyekti_posyagan_formi_provedennya_informatsiynih_viyn (дата звернення: 10.05.2022)

14. Глазов О.В. Національна безпека: сутність, ознаки, концепція та геополітичні чинники. Політологія. Наукові праці. 2011. Вип. 143, Т. 155. С. 42–46

15. Про рішення Ради національної безпеки і оборони України» від 29.12.2016 року «Про Державну програму розвитку Збройних Сил України на період до 2020 року» : Указ Президента України від 22.03.2017 № 73/2017. URL: https://www.president.gov.ua/documents/732017-21498 (дата звернення: 14.03.2021).

16. Про Рішення Ради національної безпеки і оборони України» від 02.11.2019 року «Про Міжвідомчу комісію з питань оборонно-промислового комплексу» : Указ Президента України від 08.11.2019 № 831/2019. URL: https://www.president.gov.ua/documents/8312019-30377 (дата звернення: 14.03.2021).

17. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с.

18. Про Концепцію Національної програми інформатизації: Закон України від 4 лютого 1998р. № 27-28, ст.182: веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text (дата звернення: 01.04.2022).

19. Інформаційні технології. Методи захисту системи управління інформаційною безпекою: веб-сайт. URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=66910 (дата звернення: 18.04.2022)

20. Спільна публікація 3 – 13, Спільна доктрина інформаційних операцій, Міністерство оборони США, 13 лютого 2006 р.: веб-сайт. URL: http://www.carlisle/ army.mil./DIME/documents/jp3_13pdf.

21. Гриняев С. Взгляды военных экспертов США на ведение информационного противоборства // Зарубежное военное обозрение. — 2001. — № 8.

22.Інформаційна атака: веб-сайт. URL: https://www.youtube.com/watch?v=2Ba-at0J4T0 (дата звернення: 18.04.2022)

23. Російські хакери атакували сайти державних органів Молдови: веб-сайт. URL: https://www.ukrinform.ua/amp/rubric-world/3472222-rosijski-hakeri-atakuvali-sajti-derzavnih-organiv-moldovi.html (дата звернення: 01.05.2022)

24. Денисенко про примусову депортацію жителів Маріуполя у Росію: Інформаційна операція: веб-сайт. URL: https://www.youtube.com/watch?v=dCYaU9jIBZs (дата звернення: 20.04.2022)

25. Психологічна війна: веб-сайт. URL: http://medbib.in.ua/psihologichna-viyna.html (дата звернення 26.04.2022)

26. Які наративи використовує кремлівська пропаганда: веб-сайт. URL: https://suspilne.media/amp/218468-aki-narativi-vikoristovue-kremlivska-propaganda/(дата звернення:17.04.2022)

27. Україна: Росія влаштувала провокацію, щоб втягнути Білорусь у війну: веб-сайт. URL: https://www.bbc.com/ukrainian/features-60679068.amp (дата звернення 11.04.2022)

28.ЩО ТАКЕ САБОТАЖ ТА ЯК СЕБЕ НЕ ВИКРИТИ: веб-сайт. URL: https://sprotyv.mod.gov.ua/2022/03/30/shho-take-sabotazh-ta-yak-sebe-ne-vykryty/ (дата звернення: 30.04.2022)

29. Лібіцький М., Що таке інформаційна війна? Університет національного оборони: Вашингтон, округ Колумбія, 1995 рік.

30. Е. Раус, Психологічні операції/Війна, Psywarrior: веб-сайт. URL: http://www. psywarrior.com/psyhist.html (дата звернення: 11.05.2022)

31. Об'єднаний паб 3-13.1 «Війна командування та управління», Міністерство оборони США, лютий 1996 р.

32. Мережеві війни: веб-сайт. URL: http://psychologis.com.ua/Cetevye_voyny.htm (дата звернення: 16.04.2022)

33. "Facebook Has More Than 600 Million Users, Goldman Tells Clients". Business Insider. January 5, 2011. Retrieved January 15, 2011. // http://www.businessinsider.com/facebookhas-more-than-600-million-users-goldman-tells-clients-2011-1.

34. Гезболлаг/Універсальний словник-енциклопедія—4-те вид. — К. : Тека 2006.: веб-сайт. URL: http://slovopedia.org.ua/29/53395/8667.html (дата звернення: 25.04.2022)
35. Отпор. Матеріал з Вікіпедії: веб-сайт. URL: https://uk.wikipedia.org/wiki/%D0%9E%D1%82%D0%BF%D0%BE%D1%80 (дата звернення: 21.04.2022)
36. Альтерглобалісти. Матеріал з Вікіпедії: веб-сайт. URL:https://www.wiki.uk-ua.nina.az/Альтерглобалісти.html (14.05.2021)
37. ЩО ТАКЕ САБОТАЖ ТА ЯК СЕБЕ НЕ ВИКРИТИ: веб-сайт. URL: https://sprotyv.mod.gov.ua/2022/03/30/shho-take-sabotazh-ta-yak-sebe-ne-vykryty/ (дата звернення: 30.04.2022)
38. «Празька весна» як «ідеологічна диверсія»: веб-сайт. URL: https://m.day.kyiv.ua/uk/article/den-planety/prazka-vesna-yak-ideologichna-dyversiya (дата звернення: 16.04.2022)
39. Нинішня війна - це й битва за право давати явищам наші імена: веб-сайт. URL: https://www.ukrinform.ua/rubric-society/3459228-ninisna-vijna-ce-j-bitva-za-pravo-davati-avisam-nasi-imena.html (дата звернення: 16.04.2022)
40. Семантична війна за незалежність: веб-сайт. URL: https://nv.ua/ukr/amp/istoriya-ukrajini-yak-ukrajincyam-osmisliti-svoyu-istoriyu-novini-ukrajini-50211237.html (дата звернення: 27.04.2022)
41. Інформаційна війна: веб-сайт. URL: uk.wikipedia.org/wiki/інформаційна_війна (дата звернення: 02.05.2022)
42. Ласвель Г. Техніка пропаганди у світовій війні: скор. пров. з англ. у обробці Н. М. Потапова. Л.: Відділ військової літератури Держвидав, 1929. 200 с.
43. Крисько В. Г. Секрети психологічної війни (цілі, завдання, методи, форми, досвід) / В. Г. Крисько. - Мн.: Харвест, 1999.
44. Росія розганяє фейки про плани Польщі щодо України – РНБО: веб-сайт. URL: https://www.unian.ua/war/rosiyska-propaganda-kreml-rozganyaye-feyki-pro-plani-polshchi-shchodo-ukrajini-novini-vtorgnennya-rosiji-v-ukrajinu-amp-11835576.html (дата звернення: 21.05.2022)

45. Найбільш вражаючі приклади інформаційних війн 21 століття: веб-сайт. URL: https://businessviews.com.ua/ru/studies/id/najbilsh-vrazhajuchi-prikladi-informacijnih-vijn-21-stolittja-2037/ (дата звернення: 01.05.2022)

46. 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

47. Дугін А. Г. Основи геополітики. Геополітичне майбутнє. Думати Простором / А. Г. Дугін. - М.: Арктогея-центр, 1999. - 928 с

48. Ласвель Г. Техніка пропаганди у світовій війні: скор. пров. з англ. в обробці Н. М. Потапова/Г. Ласвель. - Л.: Відділ військової літератури Держвидав, 1929. - 200 с.

49. Ellul J. Propaganda. The formation of men's attitudes. – New York, 1965

50. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи: веб-сайт. URL: http://justinian.com.ua/article.php?id=3222 (дата звернення: 14.04.2022)

51. Провокація: як розпізнати та знешкодити: веб-сайт. URL: https://thepoint.rabota.ua/provokatsiya-yak-rozpiznaty-ta-zneshkodyty/ (дата звернення: 28.04.2022)

52. Чутки як масовидне явище психіки: веб-сайт. URL: https://stud.com.ua/15748/psihologiya/chutki_massovidnoe_yavische_psihiki (дата звернення: 02.05.2022)

53. Інформаційно-аналітична діяльність. Моделі інформаційних війн: веб-сайт. URL:http://megalib.com.ua/content/2017_54Modeli_informaciinih_viin.html (дата звернення: 01.05.2022)

54. Почепцов Г. Г. Інформаційні війни / Г. Г. Почепцов. : Рефлбук; Київ : Вакаєр, 2000. - 576 с

55. Євромайдан: українська цифрова революція та останній шанс аналоговим політикам стати цифровими: веб-сайт. URL: https://blogs.pravda.com.ua/authors/savanevsky/5298980715e65/ (дата звернення: 29.04.2022)

56. Як захиститися від російської пропаганди у час війни: веб-сайт. URL: https://rayon.in.ua/news/501695-yak-zakhistitisya-vid-rosiyskoi-propagandi-u-chas-viyni (дата звернення: 31.04.2022)

57.Кремль розгорнув дезінформаційну кампанію про начебто «перемогу» у війні: веб-сайт. URL: https://www.ceskenoviny.cz/ukrinform/ukrajinsky/zprava.php?id=991385 (дата звернення: 12.04.2022)

58. Майже 80% росіян вірять у "нацистів", яких "підтримує" українська влада: веб-сайт. URL:https://m.gazeta.ua/articles/world-life/_majzhe-80-rosiyan-viryat-u-nacistiv-yakih-pidtrimuye-ukrayinska-vlada/1083342 (дата звернення: 19.05.2022)

59. Панарін І. Н. Інформаційна війна та геополітика. Інформаційна геополітика США/І. Н. Панарін.: Покоління, 2006.: веб-сайт. URL: http://www.ereading.ws/chapter.php/123890/38/Panarin__Informacionnaya_voiina_i_geopolitika.html

60. Фейки війни, провокації про біженців, маніпуляції «гарячими» темами: веб-сайт. URL: https://rayon.in.ua/blogs/502179-feyki-viyni-provokatsii-pro-bizhentsiv-manipulyatsii-garyachimi-temami-deza-na-volini-u-berezni (дата звернення: 01.05.2022)

61.ZВИЧАЙНИЙ РАШИZМ: ЯК ОДНА ЛІТЕРА ЗАХОПИЛА ТА НАЦИФІКУВАЛА РОСІЮ: веб-сайт. URL: https://www.volynnews.com/news/all/Zvychaynyy-rashyZm-iak-odna-litera-zakhopyla-ta-natsyfikuvala-rosiiu/ (дата звернення: 13.05.2022)

62. КАДРИ ІЗ ІРПЕНЯ, БУЧІ ТА ГОСТОМЕЛЯ ВІД ЯКИХ ХОЛОНЕ КРОВ: ХРОНІКА 39 ДНЯ ВІЙНИ: веб-сайт. URL: https://www.5.ua/suspilstvo/kadry-iz-irpenia-buchi-ta-hostomelia-vid-iakykh-kholone-krov-khronika-39-dnia-viiny-273315.html (дата звернення: 03.04.2022)

63. Основні моделі організації інформаційних війн та їх різновиди: веб-сайт. URL: http://soctech-journal.kpu.zp.ua/archive/2015/67-68/11.pdf (дата звернення: 22.04.2022)

64. Фейк як інструмент інформаційної війни: веб-сайт. URL: https://yur-gazeta.com/publications/practice/inshe/feyk-yak-instrument-informaciynoyi-viyni.html (дата звернення: 14.05.2019)

65. Фейк, вид інформаційної війни: веб-сайт. URL: http://rivne-news.com.ua/blogs/feik-jak-nstrument-nformac-ino-v-ini-pro/feik-jak-nstrument-nformac-ino-v-ini-pro.html (дата звернення: 29.04.2022)

66. Розвінчуємо міфи війни: три найновіші фейки про освіту та дітей: веб-сайт. URL: https://osvitoria.media/experience/rozvinchuyemo-mify-vijny-3-najnovishi-fejky-pro-osvitu-ta-ditej/ (дата звернення: 20.04.2022)

67. Найпоширеніші фейки або як працює російська пропаганда: що треба знати, щоб не вестись на неї: веб-сайт. URL: https://bilyayivka.city/articles/202013/poshirenishi-fejki-abo-yak-pracyuye-rosijska-propaganda-scho-treba-znati-schob-ne-piddavatis-manipulyacii (дата звернення: 29.04.2022)

68. Російська деза у час війни: фейки про АЕС, біженців та українських військових: веб-сайт. URL: https://rayon.in.ua/news/494106-raketniy-udar-po-aes-i-pereselentsi-turisti-rosiyska-deza-4-bereznya (дата звернення: 05.04.2022)

69. ЯК ЧИТАТИ НОВИНИ ПІД ЧАС ВІЙНИ: веб-сайт. URL: https://lvivmediaforum.com/news/ya/ (дата звернення: 24.04.2022)

70. Інформаційна війна як найбільш агресивна форма інформаційного протиборства: веб-сайт. URL: https://westnews.info/news/Informacijna-vijna-yak-najbilsh-agresivna-forma-informacijnogo-protiborstva.html (дата звернення: 11.05.2022)

71. Інформаційна війна як інструмент пропаганди війни: Правові підстави протидії: веб-сайт. URL: http://pgp-journal.kiev.ua/archive/2020/8/56.pdf (дата звернення: 10.04.2022)

72. Інформаційні війни: проблеми, загрози та протидії: веб-сайт. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/65/79 (дата звернення: 23.04.2022)

73.У.Ільницька, «Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам»,Політичні науки, No. 1(2), стор. 27-32, 2016.

74. Ржевська Н. Вплив інформаційного суспільства на формування категоріального апарату політичної науки: інформаційна демократія як політична категорія / Н. Ржевська // Вісник Львівського університету. Серія філософсько-політологічні студії.

- 2011. - Вип. 1. - С. 303-310. URL: http://nbuv.gov.ua/UJRN/Vlu_fps_2011_1_35. (дата звернення: 16.04.2022)