УПРАВЛІННЯ ОСВІТИ І НАУКИ
ЧЕРКАСЬКОЇ ОБЛАСНОЇ ДЕРЖАВНОЇ АДМІНІСТРАЦІЇ
КОМУНАЛЬНИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«ЧЕРКАСЬКИЙ ОБЛАСНИЙ ІНСТИТУТ ПІСЛЯДИПЛОМНОЇ ОСВІТИ
ПЕДАГОГІЧНИХ ПРАЦІВНИКІВ ЧЕРКАСЬКОЇ ОБЛАСНОЇ РАДИ»

СУЧАСНІ ІНФОРМАЦІЙНІ ВІЙНИ У МЕРЕЖЕВОМУ ОНЛАЙН–ПРОСТОРІ

навчально-методичний посібник

ЧЕРКАСИ – 2025

УДК 316.472.4

С91

Рекомендовано до друку вченою радою комунального навчального закладу «Черкаський обласний інститут післядипломної освіти педагогічних працівників Черкаської обласної ради». Протокол №5 від 27 грудня 2024 року

АВТОР−УКЛАДАЧ:

Плахута В.В., методист відділу фізичної культури, військово-патріотичного виховання та основ здоров'я комунального навчального закладу «Черкаський обласний інститут післядипломної освіти педагогічних працівників Черкаської обласної ради»

РЕЦЕНЗЕНТИ:

Монастирський В.М., доцент військової кафедри Черкаського національного університету імені Богдана Хмельницького, кандидат педагогічних наук;

Ложка В.Б., учитель предмета «Захист України» Черкаської спеціалізованої школи І-ІІІ ступенів №28 імені Т.Г. Шевченка Черкаської міської ради Черкаської області

С91 Плахута В.В. Сучасні інформаційні війни у мережевому онлайн−просторі: навчально-методичний посібник. Черкаси: ЧОІПОПП ЧОР, 2025. 116 с.

У посібнику представлено методологічні, методичні та практичні аспекти сучасних інформаційних війн у мережевому онлайн-просторі. Методологічною основою посібника є алгоритмізація процесів під час планування, реалізації та оцінки результативності здійснених інформаційно-психологічних операцій у соціальних онлайн-мережах.

Навчально-методичний посібник розрахований на вчителів (викладачів) предмета «Захист України» закладів загальної середньої освіти, осіб, що цікавляться інформаційними війнами та питаннями розвитку сучасних інформаційно-комунікаційних процесів.

ЗМІСТ

ВСТУП

Сучасне суспільство формується в контексті трьох технологічних напрямків – хай-х'юм (високі гуманітарні), хай-тек (високі технічні) та хай-сенсоро (високі сенсорно-технологічні). Вони формують характер людської спільноти початку ІІІ-го тисячоліття, що визначається як постіндустріальна, постмодерністська та цифрова.

Цифровий характер сучасних технічних комунікацій формує принципово нову модель взаємовідносин між індивідуумами на персональному, внутрішньогруповому та міжгруповому рівнях. З моменту народження, у середині ХХ ст., цифрові технології пройшли три етапи технологічного оновлення, які визначаються форматами web 1.0, web 2.0, web 3.0. Сьогодні ми знаходимося на етапі, коли працюють технології web2.0 та 3.0 та народжується 4.0. Цей етап розпочався із створення першої соціальної мережі (1995 р.) і визначається як час домінування онлайн-мережевих суспільств, деякі з них, зокрема, мають глобальний планетарний характер. Зсув значної частини життєвих процесів у віртуальний простір призвів до формування нових філософських постулатів, морально-етичних концепцій соціально-економічних та політичних управлінських систем. А також до напрацювання нових підходів та засобів ведення військових дій.

У контексті зазначених вище тенденцій, у період війни, яку російська федерація розв'язала і веде проти України, виникає нагальна необхідність переосмислення зробленого і здійснення системних заходів, спрямованих набуття сьогодні в військовій справі принципово нових рис, порівняно з усією минулою історією локальних та світових війн. Система управління віртуалізується, значна частина функцій людини перекладається на штучний інтелект та машини. В цих інноваціях особливе значення відіграють інтернет-технології, як засіб передачі даних та технічна підтримка базового інформаційного процесу.

Розвиток онлайн-соціальних мереж і глобалізація світового співтовариства активно використовуються у військовій галузі не тільки з метою здійснення управлінських процесів, але й для ведення віртуальних бойових дій, які забезпечують реальні військові протистояння.

Актуальність процесів формування системної практики ведення інформаційних війн викликала необхідність комплексної підготовки як профільних фахівців, так і додаткового навчання фахівців як важливої стратегічної ***мети*** для вітчизняних закладів освіти та центрів перепідготовки кадрів. Саме на досягнення зазначеної мети орієнтований даний навчально-методичний посібник.

1. Історія розвитку інформаційних конфліктів

Перші люди - Homo erectus з'явилися близько 3,5 млн років до н.е., і вже на той момент мали певні інформаційно-комунікаційні технології, які допомагали первісному стаду організовувати полювання, займатися збиральництвом та захищати свої групи. Це були переважно жести, міміка, тактильна комунікація та вигуки. Саме на основі вигуків відбулася подальша трансформація первісних комунікаційних технологій людства, перетворивши їх з часом на **мову** (у форматі мовлення).

Мовлення стало першою універсальною інформаційно-комунікаційною технологією, винайденою людством, яка докорінно змінила та прискорила подальшу еволюцію людства. Ця технологія із відповідними змінами та удосконаленнями проіснувала до теперішнього часу і має подальші перспективи.

Для первісної людини мовлення було важливим інструментом, за допомогою якого здійснювалося:

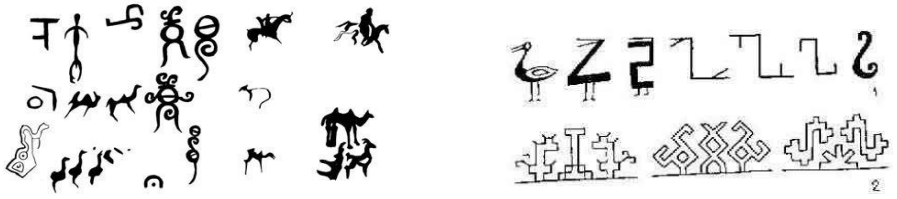
- *передання досвіду та навчання;*
- *координація спільних дій під час полювання, війни, господарчої діяльності;*
- *пізнання навколишнього середовища та міжособистісні контакти.*

Протягом X-V тис. до н.е. первісні мови почали формувати мовні родини, яких зараз налічується по світу 25.

Другим за значенням винаходом щодо розвитку інформаційно-комунікаційних технологій у первісному суспільстві стало народження **мистецтва**, яке стало графічним образно-символьним засобом передання інформації та здійснення комунікацій.

Доісторичне мистецтво можна простежити тільки за збереженими знахідкам кам'яної доби.

Поступовий розвиток образотворчого мистецтва – від перших печерних розписів та первісної пластики призвів до трансформації певних образів у символи, які несли в собі певні обсяги інформації і передавалися як у просторовому, так і в часовому вимірі (див. мал. 1).



Мал.1. **Образи та знаки первісності**

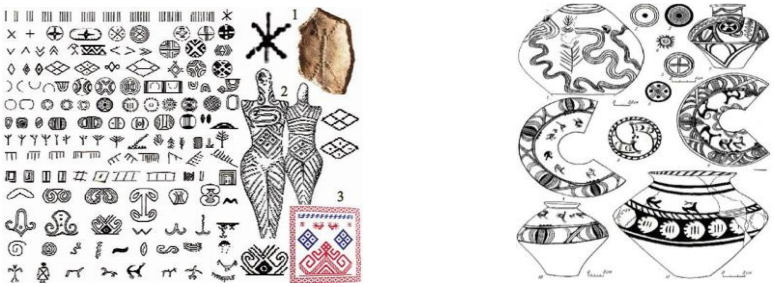
З часом образні малюнки перетворювалися на певні символи При цьому один символ міг нести інформацію як про окремий об'єкт (тварина, людина,

камінь, зброя тощо), так і про певне явище (смерть, народження, життя) або подію (полювання, свято, обряд та ін.).

На теренах сучасної України прикладами народження та розвитку первісних інформаційно-комунікаційних технологій слід вважати знахідки зразків образотворчого мистецтва на стоянці Межиріччі, наскельних малюнків та графіті Кам'яної Могили, а також система знаків та символів на кераміці трипільської культури (мал. 2.).

Мал. 2. **Зображення Кам'яної Могили**

Особливо важливою та показовою, в контексті порушеної проблематики, стала система протописемності, яку дослідники зафіксували у представників Трипільської спільноти. Фактично, це можна вважати писемністю, яка поки що не розшифрована. Втім певні смислові образи та символи трипільців все ж таки були розкриті радянським археологом Б. А. Рибаковим (мал. 3.).



Мал.3. **Символи на трипільській кераміці**

Наприкінці кам'яної доби, у так звану епоху неоліту, з'являються перші протоміста, основи виробничої економіки (землеробство та тваринництво) а також певні потужні соціальні об'єднання, які потребували певних символьно-образних систем для здійснення класичного інформаційного процесу – створення, накопичення, збереження та поширення інформації. Остаточно зазначені системи сформувалися вже на наступному етапі.

Підсумовуючи інформаційно-комунікаційні здобутки первісної епохи, слід окреслити її найбільш характерні ознаки.

Основними типовими прикладами первісних *інформаційних війн* можна вважати сакральну боротьбу (первісна магія) із силами природи та тваринами, а також на рівні внутрішньоплеменних та міжплеменних конфліктів. Останні супроводжувалися не тільки магічними обрядами, але й першими інформаційними атаками у вигляді залякування, дезінформації, приховування та інших типових для базового рівня інструментів.

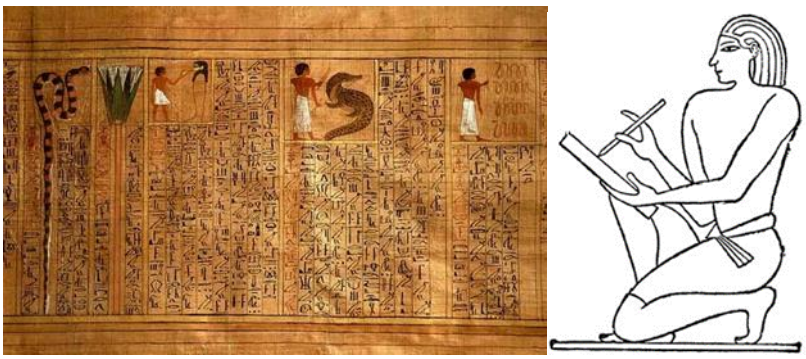
Головними *інформаційними носіями* для первісної людини слугували побутові речі, твори мистецтва, зброя та прикраси з кістки та шкіри тварин, дерев'яні речі, посуд (глина та дерево), каміння (окремі вироби, валуни, стіни печер).

Як таких центрів або чітко визначених виробників інформації виокремити важко. Знання та досвід, що передавалися з покоління в покоління, накопичувалися колективно. Можливо, твори первісного мистецтва були прерогативою шаманів, утім чітких підтверджень цьому немає.

Поява великих соціальних об'єднань (протоміста та ранні міста, іноді налічували 10-15 тис. мешканців) призвела до необхідності формування певних регламентуючих систем, згідно з якими відбувався чіткий розподіл праці, повноважень, прав та обов'язків. Так сформувалися перші міста держави у долинах річок Інд (Мохенджодаро), міжріччі Тигру і Єфрату (Месопотамія) та Нілу (Давньоєгипетська держава).

Важливою складовою частиною державного устрою зазначених утворень є певні універсальні управлінські системи, що базувалися на конкретних інформаційно-комунікаційних технологіях. Це призвело до остаточної трансформації малюнкової образно-знакової системи передання відомостей та даних на перші, **ієрогліфічні писемні системи.** Цю подію можна ідентифікувати як типову інформаційну революцію з усіма її відповідними ознаками.

Подальша трансформація первинних письмових систем призвела до виникнення його еволюційного продовження – **абеткової писемності**. Ця система була більш гнучкою та універсальною і вже від неї походять всі письмові системи епохи Античності. Писемність надала інформаційному процесу конкретність, чіткість та змістовність. З'явилась можливість для надійного збереження та ефективного поширення інформації.



Мал.4. **Давньоєгипетська писемність**

На цьому етапі в Давньому Єгипті було винайдено більш універсальний, порівняно з традиційними, інформаційний носій – папірус з чорнилами (мал. 4). Така форма фіксації інформації не вимагала значних зусиль, її було простіше зберігати, вона була більш мобільною.

Під час військових дій вожді та полководці застосовували практику залякування, психологічного тиску, дезінформації, спрямовані проти ворогів, а також методи стимулювання, підбадьорювання власних воїнів.

Одним із нових інструментів, що з'явився саме за часів античності, є **реклама**. Первинна реклама функціонувала у вигляді системи аудіо та текстових оголошень – перші здійснювалися з допомогою глашатаїв, іноді − у вигляді тематичних пісень та віршів, другі наносилися на стіни будинків (на спеціально побілених для цього стінах «амбусах»). У цілому така комунікація носила достатньо мирний характер – у вигляді оголошень про продажі, збори, гладіаторські бої, повідомлення особистого характеру (мал.5).

Мал. 5. **Рекламні написи у Помпеях**

Втім іноді такі повідомлення виконували функцію інформаційної зброї.

Зокрема, в місті Помпеї були зафіксовані написи, котрі можна трактувати як дискредитацію, компромати або позитивні відгуки на певних персон, які обиралися на посади в міські магістрати. Також глашатаї могли вигукувати заклики до певних дій або звинувачення проти певних осіб.

Інформаційне супроводження міжнародних подій – військових конфліктів, дипломатичних стосунків, міжнародної торгівлі здійснювалося за допомогою

певних демаршів, надання дезінформації шляхом шантажування ворожих лідерів.

Приблизно у цей час (500 рр до н.е.) в Китаї військовий стратег Сунь Цзи написав свій трактат «Мистецтво війни», в якому показав, як потрібно застосовувати елементи інформаційної війни, а деякі вказівки взагалі можна віднести до гібридних воєн, а саме:

- висміювати та дискредитувати все цінне і добре, що є в країні ворога;
- втягувати видатних представників противника у злочини;
- підривати імідж національних лідерів та виставляти їх на загальний осуд;
- залучати до співпраці підлих та мерзотних людей;
- розпалювати сварки та провокувати конфлікти у населення ворожої країни;.
- підбурювати молодь проти старих;
- заважати діяльності влади;
- підривати міць війська;
- знецінювати традиції та національні цінності;
- розбещувати населення;
- застосовувати підкуп, стимулювати корупцію.


Мал. 5. **Сунь Цзи та його «Мистецтво війни» (набамбукових дощечках)**

У плані супроводження військових дій Сунь Цзи радив активно застосовувати дезінформацію, залякування, психологічний тиск та інші традиційні методи.

Тогочасні інформаційно-комунікаційні технології активно застосовували античні політики. Зокрема, в Давній Греції їх активно практикував оратор Демосфен у процесі боротьби з македонським царем Філіпом, який завоював грецькі міста-держави. З допомогою публічних виступів, дискусій, діалогів досягали своїх цілей афінські політики Солон, Фемістокл, Перикл.

Саме в Давній Греції виникла нова професія − софістика, представники якої спеціалізувалися у публічних виступах та вмінні переконувати. Це можна вважати еволюцією традиційних глашатаїв.

У Давньому Римі політики та полководці Юлій Цезар, Марк Цицерон, Марк Аврелій успішно застосовували інформаційні технології проти своїх політичних противників та зовнішніх ворогів. Наприклад, Сципіон Африканський, активний прибічник війни з Карфагенською державою, кожний свій виступ в Сенаті закінчував фразою: «Втім, Карфаген має бути знищений». Цей прийом – багатократне повторення певної тези й сьогодні активно використовується.

Література, зокрема сатиричні твори, також використовувалися в якості інформаційної зброї, спрямованої проти конкретних персон або для впливу на колективну свідомість.

Підсумовуючи інформаційно-комунікаційні здобутки епохи ранніх держав та Античності, слід окреслити її найбільш характерні ознаки.

Базовий *інформаційний процес* у первісному суспільстві відбувався шляхом створення (дослідження навколишнього світу, наукового пізнання та перетворення умов зовнішнього середовища), фіксації (мистецтво, архітектура, реклама, писемність) та передання (мовлення, мистецтво, реклама, писемність) інформації.

Головними *інформаційними носіями* для первісної людини слугували кістки та шкіра тварин, дерев'яні речі, посуд (глина, дерево, метал, скло), каміння (окремі вироби, статуї, скелі), з'являється і набуває значного поширення папірус. Основними типовими прикладами *інформаційних війн* епохи ранніх держав Сходу та Античності можна вважати класичні, в сучасному розумінні, інформаційно-психологічні операції. Останні супроводжували військові конфлікти, політичні та економічні, а також релігійні процеси.

В епоху ранніх держав та античності виробництво контенту поступово виокремлюється в окремий напрям діяльності, який охоплює мистецтво, релігію, військову справу, державне управління, а також науку, яка народжується в ці часи. Тепер створенням, накопиченням та поширенням інформації займаються чітко визначені соціальні групи. Саме жерці та вчені були в переважній більшості виробниками інформації.

Храми та світські школи стають своєрідними *фабриками контенту*, який продукується відповідно до специфіки та тематики діяльності її виробників. Значні обсяги інформації накопичуються у перших бібліотеках (Шумер, Вавилон, Олександрійська в Єгипті та ін.). Також в якості центрів створення інформації були адміністративні структури – царські канцелярії, муніципальні управління, військові структури, торгові об'єднання.

Доволі значний внесок у практику ведення інформаційних війн внесла Візантійська імперія. Зокрема, ми знаємо багато історичних фактів, коли візантійські імператори перемагали свої ворогів не силою зброї, а шляхом

дезінформації, психологічного тиску, підкупу. Особливо активно велися такі війни у протистояннях із князями Київської Русі, ісламськими державами, кочовими племенами давніх тюрків та ін.

Серед визначних теоретиків та практиків інформаційних війн можна виділити Маврикія та його твір «Стратегікон», Костянтина Багрянородного, а також окремий анонімний документ «Риторика мелітаріс» (збірка військових промов та настанов).

Певні прийоми та засоби ведення інформаційної війни від візантійців запозичили керманичі Київської Русі, додав до цього аналогічний досвід варягів, створивши таким чином свою систему. Зокрема інформаційно-комунікаційні технології в Давньоруській державі застосовувалися, як у внутрішньополітичних процесах, так і під час збройних конфліктів. Активну участь у цьому брала православна церква.

Серед відомих київських князів практикували такі технології під час військових походів та при вирішенні внутрішньополітичних проблем − Святослав, Ольга, Володимир Великий, Ярослав Мудрий та Володимир Мономах.

У часи Середньовіччя та Відродження розвиток усіх аспектів суспільства відбувається під безпосереднім контролем та за участі церкви. Саме цей соціальний інститут, більш ніж на тисячоліття стає провідним споживачем та розробником інформаційно-комунікаційних технологій, а також активним учасником тогочасних інформаційних війн.

Медіатехнології цього часу базуються на таких традиційних інструментах, як: мова, мистецтво, писемність, реклама, література. Разом з тим з’являються нові, як то: **пропаганда** та **психологічна війна.**

У часи боротьби католицької церкви з Реформацією при Ватикані було створено «Конгрегацію пропаганди віри» (1622 р.), яка була фактично першим історично зафіксованим центром підготовки та проведення інформаційно-психологічних спецоперацій.

Церква воювала з Реформацією традиційними та відпрацьованими століттями інструментами – використовували мережу храмів, монастирів та церковних орденів, непорушний авторитет «Біблії», папського престолу, авторитет єпископів, архієпископів, кардиналів, настоятелів монастирів. Активно залучалися всілякі божественні дива, маніпуляція історичними та науковими фактами. У цій боротьбі дуже активно себе проявила «Конгрегація пропаганди віри».

В епоху формування та первинного розвитку ринкових капіталістичних відносин інформаційні війни виконували функцію допоміжної технології із супроводження збройних конфліктів та економічних війн. Завдяки

запровадженню європейцями нових технологій та поширення їхнього впливу на інші континенти, центри розвитку інформаційно-комунікаційних технологій формуються далеко за межами Європи. Зокрема, одним з провідних стала колоніальна, а потім незалежна Північна Америка.

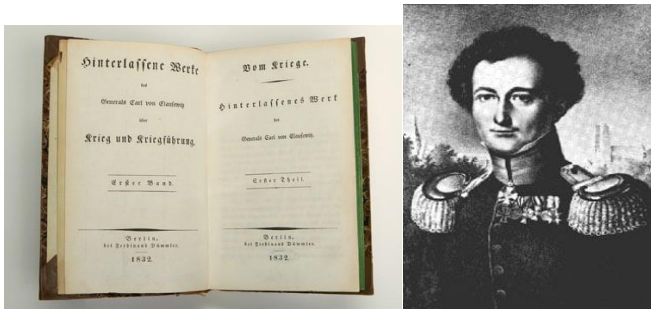
У своїй боротьбі колоністи використовували соціальні мережі (товариства «Сини свободи», «Кореспондентські комітети»), застосовували образні символи («Дерево свободи»), стереотипи та лозунги («Воля або смерть»). Вони дуже активно застосовували дієві акції, тогочасні медіа, чутки, маніпуляцію.

Головним інструментом ведення інформаційних війн перша французька республіка та Наполеон вважали соціально привабливі ідеї свободи, рівності економічного та політичного прогресу, що розповсюджували у суспільствах монархічних країн, з якими вони вели війни. Французькі емісари підривали внутрішню міць та єдність противника, формували мережі агентів впливу, підбурювали до спротиву та створення опозиційних організацій і медіа.

Усі провідні світові конфлікти XIX ст. обов'язково супроводжувалися інформаційними протистояннями із застосуванням такого інструменту, як **преса,** що **стала другою глобальною мас-медіа технологією**. Сам цей термін походить від назви першої масової газети «La Presse», що почала видаватися у 1831 р. З цього моменту специфіка та особливості ведення інформаційних війн набувають специфічного характеру. Преса стає інструментом масового впливу на свідомість суспільства, а відповідно засобом маніпуляції, дезінформації, залякування, стимулювання, заклику та інших засобів ведення інформаційних війн.

Наприкінці XIX століття з'являється нова інформаційно-комунікаційна технологія – **радіо** (Марконі, 1895), яка з часом перетворилася на потужну **третю глобальну мас-медійну технологію.**

Серед теоретиків та практиків інформаційних війн зазначеного періоду важливе значення мали розробки прусського генерала Карла Фон Клаузевіца, викладені в його книзі «Про війну» (1832 р.). На його думку, однією з головних складових успіху будь-якої армії є «відчуття перемоги», тобто, переможна психологія, дух, мораль. Вони є головною мішенню та об'єктами, по відношенню до яких діють інформаційно-комунікаційні атаки противника (мал. 6).



Мал. 6. **Генерал К.Клаузевіц та його книга «Про війну»**

У форматі нашої тематики особливе значення мають такі його постулати, які можуть бути трактовані й навіть як базові для гібридної війни:

- ⇒ **БИТВА** – це не тільки знищення живої сили ворога, а й знищення його мужності.
- ⇒ **ЗАКОЛОТ** у суспільному та державному устрої набагато легше відбувається в умовах загального потрясіння та прискореного розвитку, які приносить війна.
- ⇒ **ТІ, ХТО НЕ ПАМ'ЯТАЮТЬ ВЛАСНОГО МИНУЛОГО,** приречені на його повторення.

Узагальнюючи інформаційно-комунікаційні здобутки епохи раннього капіталізму, визначаємо наступні характерні ознаки.

Базовий *інформаційний процес* у XVII-XIX ст. відбувався шляхом створення (дослідження навколишнього світу суспільних процесів, наукового пізнання та перетворення умов зовнішнього середовища), фіксації (наука, мистецтво, архітектура, реклама, писемність) та передання (мовлення, мистецтво, реклама, писемність, ранні медіа) інформації.

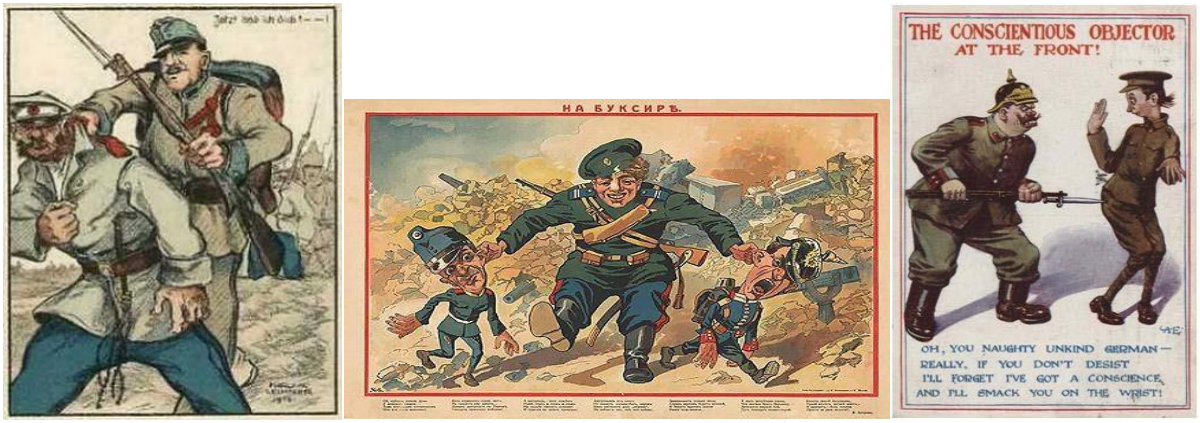
Головними *інформаційними носіями* для людини в ці століття були передусім книжки, офіційна документація, листи – на основі паперу, твори мистецтва – папір, тканина та інші, характерні минулим епохам. Основними прикладами *інформаційних війн* цього періоду можна вважати типові, в сучасному розумінні, інформаційно-психологічні операції (залякування, дезінформація, психологічний тиск та ін.). Останні супроводжували військові конфлікти, політичні та економічні процеси.

Виробництво контенту є окремою спеціальністю, яка забезпечує необхідними даними економічні процеси, мистецтво, військову справу, державне управління, науку, релігію. Створенням, накопиченням та поширенням інформації займаються чітко визначені фахівці.

ФАБРИКАМИ КОНТЕНТУ стають навчальні заклади, наукові центри, адміністративні структури, безпосередньо медіа.

На початку XX ст. більш-менш сталий світовий порядок, який формувався століттями, було порушено. Відбулася низка потужних революцій (Росія, Німеччина, Австрія, Латинська Америка, Далекий Схід та Південна Азія), а також дві світові війни. Потім майже до кінця століття світ знаходився у форматі двополярного протистояння (США-СРСР).

Першим прикладом найбільш успішного застосування технологій інформаційної війни в XX ст. стало виведення з числа активних учасників Першої світової війни Росії та розвал Російської імперії (мал. 7).



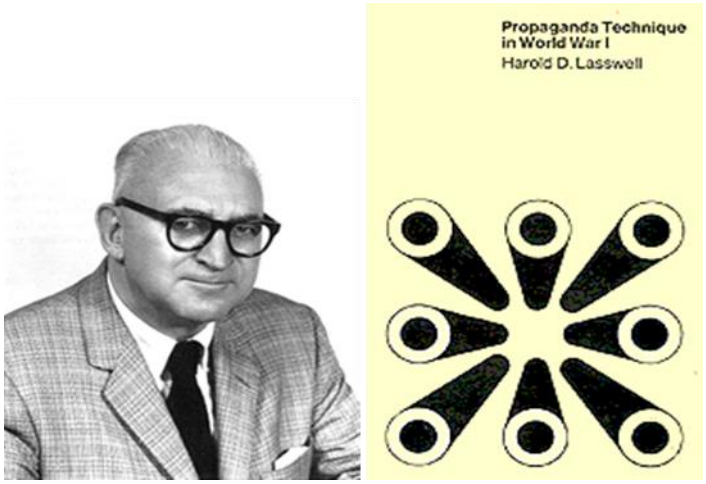
Мал. 7. **Агітаційні плакати часів І-ї Світової війни**

Розуміючи міць Антанти (союз Англії, Росії, Франці та США та в цілому 34 держави) і неможливість прямої перемоги Німеччини та її союзників (Австро-Угорщина, Болгарія, Туреччина), уряд Кайзера Вільгельма почав стимулювати революційні рухи в Росії та, зокрема, допоміг здійснити заколот і прийти до влади Леніну та очолюваній ним партії більшовиків. У результаті цієї спецоперації один з найпотужніших учасників Антанти – Росія вийшла з війни та розпочала боротьбу із своїми колишніми союзниками.

Проте, значної переваги Німеччині ця перемога не дала. Антанта таки перемогла, в Німеччині, а також у її союзника Австро-Угорщини відбулися революції, які призвели до розвалу цих імперій і утворення республік з більш-менш демократичними режимами.

Одним з перших питання розвитку інформаційно-комунікаційних технологій та інформаційної війни в XX ст. почав системно досліджувати Г.Д.Лассуел (1902-1978). Він активно залучав методи соціальної психології, психоаналізу, психіатрії для дослідження політичної поведінки та пропаганди, виокремлюючи роль масових комунікацій в процесі ведення інформаційних протистоянь між провідними країнами світу. Саме Лассуел першим провів аналіз здійснення пропаганди під час Першої світової війни. Свої розробки він узагальнив у роботі «Техніка пропаганди у світовій війні» (1927 р.), де вперше було виділено інформаційно-психологічну сферу війни, а пропаганду подано як

особливий вид зброї, що впливає на моральний стан ворога (мал. 8).



Мал. 8**. Г.Лассуєл та перше видання «Техніка пропаганди у світовій війні»**

Народжена в горнилі Першої світової війни Радянська Росія, що з часом перетворилася на неоімперську державу СРСР, з перших днів свого існування активно застосовувала інформаційно-комунікаційні технології ведення внутрішніх та зовнішніх війн (мал. 9).

Мал. 9**. Агітаційні плакати перших десятиліть СРСР**

Внутрішня інформаційна війна велася в СРСР проти політичної опозиції (Троцький, Зинов'єв, Каменєв, Бухарін), широких незалежних соціальних верств населення (заможні селяни, інтелігенція, духовенство), національних об'єднань. У цьому контексті застосовувалися агітація, дискредитація, маніпулювання, залякування, впровадження певних психологічних установок. Жертвами цієї війни стали мільйони невинних громадян, її наслідками − створення великого державного концтабору, який охопив 1/6 світу.

Зовнішню інформаційну війну очільники СРСР проводили проти іншого цивілізованого світу, і в першу чергу проти своїх політичних та економічних конкурентів, якими в різні часи були Німеччина, США, а також міжнародні торговельно-економічні (СОТ, ЄС) та військові (НАТО) союзи.

Інформаційні атаки супроводжували відкриті та приховані конфлікти, в яких брала участь СРСР. Серед них війна з Польщею (1920 р.), Фінляндією (1939-1940 рр.) гітлерівською Німеччиною (1941-1945 рр.), участь у Корейському конфлікті (1950-1953 рр.), війні у В'єтнамі (1973-1975) Афганської війни (1979-1989 рр.), багатьох збройних конфліктах у Африці та Латинський Америці (мал.10).

Мал.10. **Агітаційні матеріали епохи радянського соціалізму**

Весь час свого існування СРСР перебувала в стані інформаційної війни, що дозволило відповідним структурам – КДБ, ЗМІ, партійним та радянським громадським організаціям напрацювати величезний досвід та сформувати дієвий інструмент ведення не тільки інформаційної, але й гібридної війни.

Найбільш потужним суперником СРСР та його союзників (так званий соціалістичний табір – військовий «Варшавський союз», економічний СЕВ) були **США та його союзники (СОТ, НАТО тощо).**

Пройшовши Першу та Другу світові війни, оволодівши ядерною зброєю, Америка стала потужним центром геополітичного впливу і поділила весь світ з СРСР на власні зони впливу. Це протистояння отримало назву «Холодна війна» (1946-1991рр.). Остання полягала у постійних інформаційних протистояннях, гонці озброєнь та економічному протистоянні в боротьбі за джерела сировини та ринки збуту.

Захищаючи власні військові, політичні та економічні інтереси, США протягом XX ст. брала участь в усіх значних регіональних конфліктах у Латинській Америці, на Близькому Сході, в Європі, Південній та Східній Азії, Африці. В переважній більшості випадків **головним опонентом був СРСР.** Жорстке протистояння двох геополітичних гігантів не одноразово ставило світ на край реальної гарячої війни.

Такими були Карибська криза (1962 р.), Берлінська криза (1961 р.), а також низка менш відомих конфліктів.

Основними центрами планування та ведення інформаційних війн у США стали Державний департамент (дипломатичне прикриття операцій), ЦРУ (планування та реалізація спецоперацій), Пентагон (військово-політичні

операції) та низка різноманітних профільних дослідницьких центрів та громадських об'єднань.

Найбільш успішною інформаційною кампанією для США стало фінальне протистояння «Холодної війни», яке прискорило процеси, що призвели до розвалу СРСР. Головною діючою особою цього протистояння став 40-й американський президент **Рональд Рейган** (1981-1989 рр.). Останній оголосив ще в 1979 р. хрестовий похід проти «Імперії Зла» і розпочав безкомпромісну економічну та інформаційно-психологічну війну з СРСР та його союзниками (мал. 11).

Мал. 11.**«Імперія зла» та «Зоряні війни» Р.Рейгана**

Головними складовими частинами боротьби Рейгана стала **економічна складова** – зниження світових цін на нафту, продаж якої був на той час чи не найголовнішою статтею прибутку СРСР, та низка економічних санкцій. Разом з тим було активізовано гонку озброєння, яка суттєво спустошила економічний потенціал Радянського Союзу.

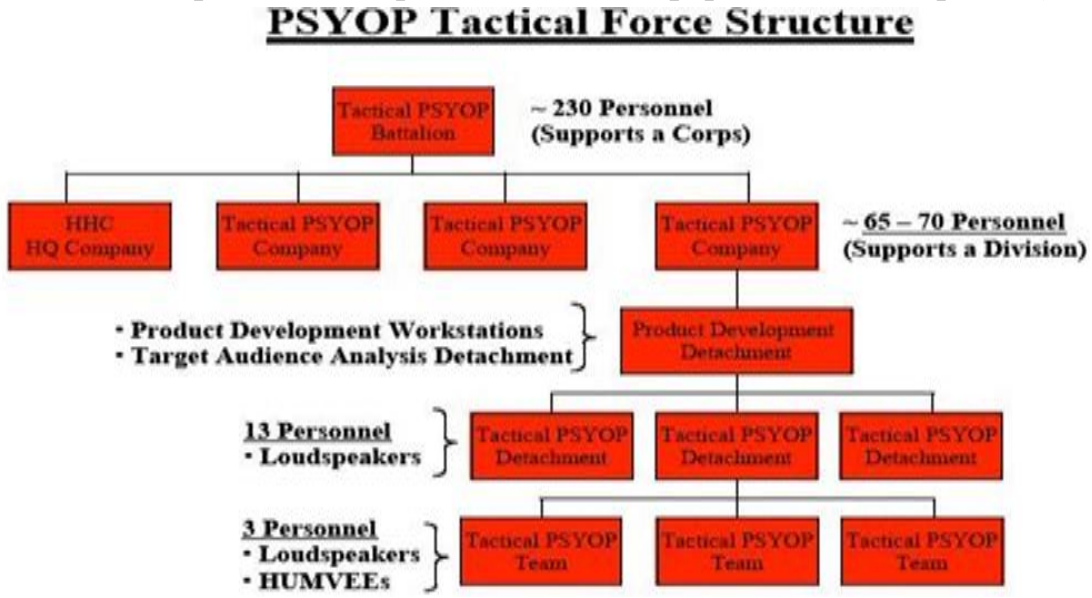
Активно використовувалася й ідеологічна складова. В 1983 році Рейган оголосив запуск програми «Стратегічна оборонна ініціатива», сутність якої полягала в тому, що американські супутники за допомогою лазерних пристроїв мали можливість знищувати будь-які ядерні ракети, націлені на Америку та її союзників ще на старті. Навколо цього проєкту було багато галасу, дезінформації, відвертих маніпуляцій. Долучився до цього навіть Голівуд, де зняли блокбастер «Зоряні війни» (1970-80-ті рр.). Також багато інформації було навколо так званої кліматичної зброї.

Загнавши шляхом економічного та інформаційно-психологічного тиску нового радянського лідера Михайла Горбачова в глухий кут, Америка змусила його розпочати перебудову та підписати низку мирних угод із Заходом, що дорівнювалося до капітуляції. Так було знищено пресловуту «Імперію Зла».

Починаючи з 1991 р., США стає фактично гегемоном у плані світової геополітики та перебудовує світову систему безпеки та економічних відносин під свої потреби та потреби своїх союзників.

Без особливих складнощів США вирішують конфлікти під час війни в Перській затоці (1990-1991 р.), війни на Балканах (1991-1999 рр.), що призвела до розпаду Югославії. Потім була війни в Іраку (2003 р.).

Під час цих конфліктів остаточно сформувалася **сучасна базова американська доктрина ведення інформаційно-психологічної війни** другого покоління, з'явилися спеціалізовані стратегії, методики, інструменти. Було створено окремі військові підрозділи психологічних операцій PSYOPS (Psychological Operations) або з 2010 р. – центри інформаційного забезпечення MISO (Military Information Support Operation). Сам **термін «інформаційна війна»** почав офіційно вживатися з 1992 р., а у 1993 р. було надане розширене тлумачення цього терміну. Базовим документом для регулювання питань проведення інформаційної війни стали Польовий Статут армії США FM-106 «Інформаційні операції» і Доктрина спільних інформаційних операцій (мал. 12).



Мал. 12. **Структура типового підрозділу із інформаційно-психологічних операцій**

Інформаційні війни XX ст. в якості базових інструментів роботи використовували як традиційні медіа, що було напрацьовано у попередні часи (друк, преса, радіо), так і нові: **кіно, телебачення**, **Інтернет**. Ці комунікаційні інструменти суттєво підвищили ефективність інформаційно-комунікаційної діяльності у рамках військових конфліктів. А два з них – телебачення та Інтернет перетворилися, відповідно, на **четверту** та **п'яту глобальні мас-медіа технології.**

Розробки Мак-Люена, що з'явилися в середині XX ст., значною мірою вплинули на формування сучасного розуміння ролі та значення цифрових медіа в контексті інформаційних конфліктів. Серед тих, хто формував теоретичні та методологічні основи сучасних інформаційних війн, особливої уваги заслуговують розробки американського політолога та соціолога З.Бжезінського

«Велика шахівниця», що вийшла в 1997 р. на стала підручником для сучасних політологів (мал. 13).

Мал.13. **Бжезінський та його бачення сучасної геополітичної стратегії**

Аналізуючи сучасний світ, його глобальні тренди та регіональні особливості розвитку, він спрогнозував та сформулював роль і значення США на глобальному просторі, місце і перспективи Росії, Китаю та інших провідних гравців світу. Зокрема, щодо ролі місця на світовій геополітичній мапі України він визначив: «*Україна – новий і важливий простір на євразійській шахівниці, вона є важливим геополітичним центром, тому що саме її існування як незалежної держави допомагає трансформувати Росію. Без України Росія втратить статус євразійської імперії. Без України Росія ще може поборотися за імперський статус, утім вона буде азійською державою*».

Наприкінці XX ст. на початку XXI ст. людство переходить у цифрову епоху, значна частина життя віртуалізується. Разом з тим інформаційні протистояння переносяться в Інтернет. Особливого значення набуває таке явище як **кібервійна.**

Остання стає важливою частиною «гарячої» війни, виконуючи функцію забезпечення та надання суттєвих переваг в реальному протистоянні.

Народження та впровадження нових технологій ведення інформаційної війни не впливає на її традиційні складові частини та цілі. Так само, як і у XX та XIX ст. або в попередні віки, головним завданням є отримання суттєвих переваг у забезпеченні військових, економічних та політичних конфліктів. Незмінність цих постулатів продемонстрували останні міжнародні конфлікти, ініціаторами яких стала Російська федерація.

Ліберальна єльцинська епоха в Росії закінчилася приходом до влади ставленика олігархічно-кланових та колишніх структур КДБ – **Володимира Путіна.** Почали лунати реваншистські заяви, розпочалася мілітаризація суспільства, збільшення виробництва зброї та активізація зовнішньополітичної агресії.

Ще з минулих часів у спадок путінській росії залишилися конфлікти в Абхазії, Чечні та Придністров'ї. До цього додали війну з Грузією, анексію Південної Осетії (2008 р.) та війну с Україною (2014-2015 р.) з анексією Криму та створенням в Донбасі терористичних об'єднань так званих «Донецької народної республіки» та «Луганської народної республіки». Крім того, РФ втрутилася в конфлікт на території Сирії, де урядові війська Асада Башара воюють із військовими угрупованнями ІДІЛ («Ісламська держава Іраку та Леванту») та місцевих повстанців.

У зазначених конфліктах Росія застосувала останній досвід вдалих інформаційно-психологічних війн, що велися США та найбільш сучасні інформаційно-комунікаційні технології. Останнє дало режиму Путіна певну тактичну перевагу та тимчасові перемоги, але в стратегічній перспективі затягло його в таку ж саму геополітичну пастку, в яку свого часу затягнув Рейган СРСР.

Слід зазначити, що інформаційній складовій у зовнішній та особливо внутрішній політиці Росія приділяє чи не головну увагу та фінансує медіа проекти по першій категорії.

Важливим здобутком XX-XXI ст. у плані розвитку інформаційно-комунікаційних технологій стало народження мережевих онлайн та оф-лайн структур. Особливо важливе значення мали онлайн структури – соціальні мережі формату WEB 2.0.

Виникнення Інтернету (1957 р. – прототип, 1991 р. − глобалізація) надало поняттю «соціальна мережа» нового значення та відкрило перед людством великі перспективи. Вже у 1995 р. **Ренді Конрадс** створює перший віртуальний соціальний мережевий ресурс і дає йому назву - **Classmates.com** - (охоплює переважно США та Канаду). Головною метою цього проєкту Конрадс вбачав надання зареєстрованим користувачам допомоги у встановленні та підтримці зв'язків з друзями та знайомими, з якими вони перетиналися протягом всього життя. Через певний час з'явилися нові мережі- **Friendster** (2002 р.), **Linked ln** (2003 р.), **MySpace** (2003 р.), **Tribe** (2003 р.), **Hi5** (2003 р.).

У 2004 році з'являються такі соціальні мережі як **Orkut**,**Bebo**,**Yahoo 360**.У цьому ж році студент Гарвардського університету Марк Цукерберг створив **Facebook**, мережу, яка зараз є безумовним лідером (в середньому кожен сьомий мешканець планети є її користувачем). На території країн СНД першими були такі соціальні мережі, як **Мой круг (**2005 р.) **Odnoklassniki.ru (**2006 р.**)** і **VKontakte.ru (**2006 р.).

Узагальнюючи інформаційно-комунікаційні здобутки XX-XXI ст., в плані розвитку інформаційних війн визначаємо **наступні характерні ознаки:**

1. ***Базовий інформаційний процес*** у цей період та наш час відбувався шляхом створення (дослідження навколишнього світу суспільних

процесів, наукового пізнання та перетворення умов зовнішнього середовища), фіксації (наука, мистецтво, архітектура, реклама, писемність) та передання (мовлення, медіа, мистецтво, реклама, писемність) інформації.

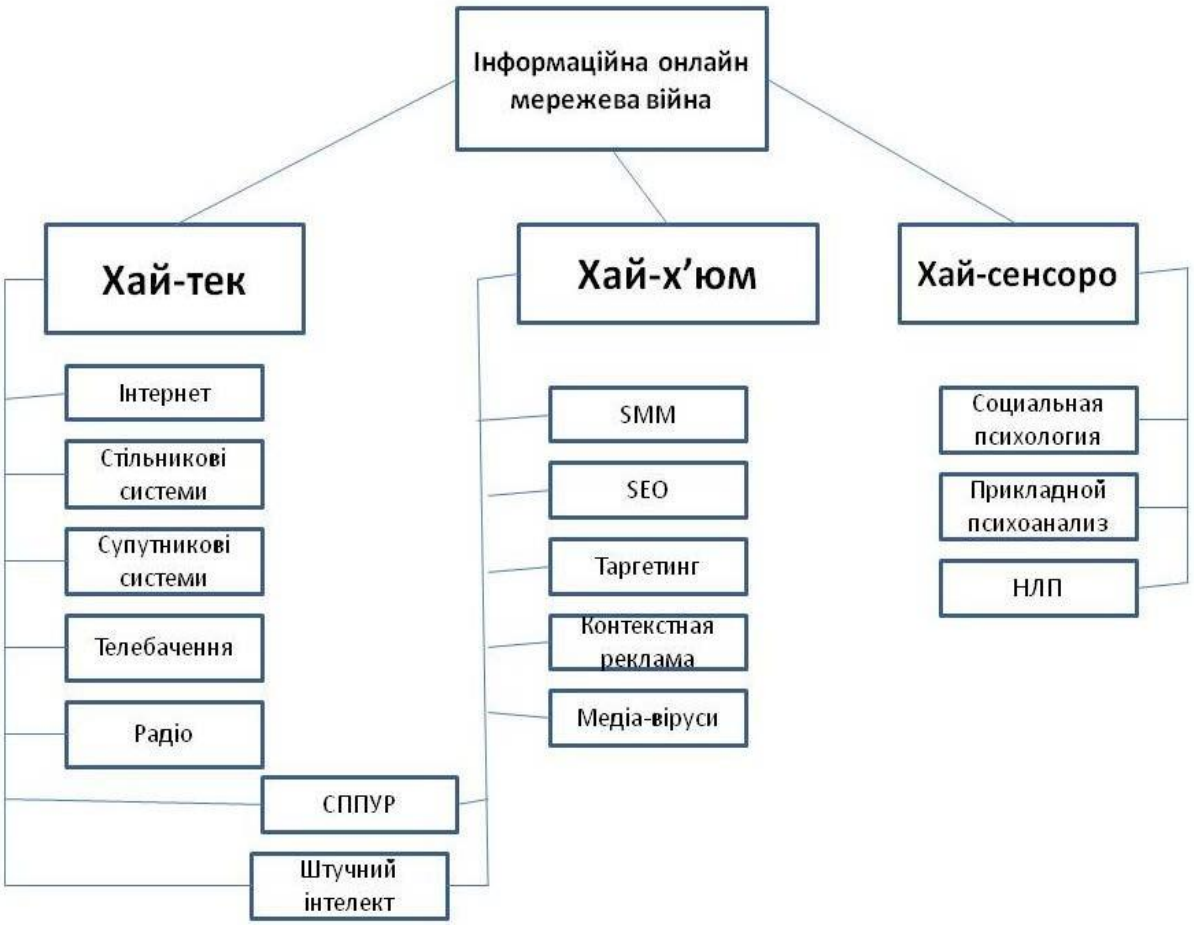
2. **Головними інформаційними носіями** для людини сьогодні є цифрові пристрої, друковані книжки, офіційна документація, персональні листи – на основі паперу, твори мистецтва – віртуальні площини, папір, тканина та інші, характерні ще минулим епохам.
3. **Основними типовими прикладами інформаційних війн** цього періоду можна вважати цифрові віртуальні конфлікти та реальні інформаційно-психологічні операції. Вони супроводжують військові конфлікти, політичні та економічні процеси.
4. **Виробництво контенту** стає чи не найголовнішою функцією суспільства, що забезпечує необхідними матеріалами економічні процеси, мистецтво, військову справу, державне управління, науку, релігію тощо. Створенням, накопиченням та поширенням інформації займаються практично всі, хто бере участь у соціальних процесах.
5. **Фабриками контенту** стають наукові центри, військові структури, навчальні заклади, адміністративні структури, безпосередньо медіа.

2. Теорія інформаційної війни: методологія та понятійний апарат

Ключовим елементом у теоретичній моделі є поняття **інформаційна онлайн мережева війна** (ІОМВ)**,** що визначається, як комплекс інформаційних впливів між соціальними системами (групами), що орієнтовані на отримання певних переваг у економічних, військових, політичних, культурних та громадських протистояннях.

У своїй основі ІОМВ має три ключові технологічні аспекти: хай-тек, хай-х’юм та хай-сенсоро. Кожен з цих аспектів має власні технології, які формують профільні напрямки дослідження та практичної роботи (див. мал. 14.).

Хай-тек в ІОМВ – сучасні високі технології цифрових комунікацій, що в основі мають системи телебачення, радіо, Інтернет, месенджерів, стільникової, супутникової та інших видів сучасного зв’язку та базуються на таких гаджетах, як стаціонарні комп’ютерні пристрої, планшети, смартфони, пристрої індивідуального та групового зв’язку.



Мал.14.Модель інформаційної онлайн мережевої війни

До цього аспекту відноситься класичне *телебачення,* в ефірному та цифровому форматах. Останнє визначають, як технологію трансляції телевізійного зображення та звуку за допомогою кодування відеосингалу та сигналу звуку із використанням цифрових каналів за стандартом MPEG.

Радіо, як класичне електронне ЗМІ, розглядається у традиційному аналоговому (АМ, FM)та цифровому форматах. Останній визначається, як технологія трансляції сигналів радіостанцій в цифровій формі за допомогою електромагнітних хвиль радіодіапазону.

Інтернет, в контексті досліджуваної теми розглядається, як всесвітня система об'єднаних комп'ютерних мереж для зберігання та транслювання інформації. На основі цієї мережі, як комунікаційної платформи формуються типові поштові сервіси, сервери зберігання даних, а також нові формати мережевого телебачення та радіо.

При цьому *інтернет-телебачення* визначається, як телебачення між мережевого протоколу (on-line TV)— система, що базується на двосторонньому цифровому переданні телевізійного сигналу через інтернет- з'єднання за допомогою широкополосного підключення.

Інтернет-радіо або веб-радіо, визначають як групу технологій трансляції потокових аудіоданих через мережу Інтернет для здійснення широкої трансляції програм. Також, в якості терміну інтернет-радіо визначається радіостанція, що використовує для трансляції технологію потокового віщання у глобальній мережі Інтернет.

Месенджери – мережі миттєвого з'єднання. Типовими прикладами таких технологій є WhatsApp, Facebook Chat, Hangouts (Google), Skype, LINE, WeChat, Viber, Kik, Snapchat, ICQ, Telegram.

Стільниковий зв'язок – один з різновидів мобільного зв'язку, в основі якого закладено стільникову мережу. Ключова особливість полягає в тому, що спільна зона покриття поділяється на ланки (соти), що визначаються зонами покриття окремих базових станцій. Соти частково перекриваються, створюючи мережу.

Супутниковий зв'язок (радіо та телебачення)−один з різновидів космічного радіозв'язку, що базується на використанні штучних супутників в якості ретрансляторів. Цей зв'язок здійснюється між наземними станціями, що є стаціонарними або мобільними. Супутниковий зв'язок є продовженням розвитку традиційного радіорелейного зв'язку шляхом винесення ретранслятора на велику висоту.

Хай-х'юм в ІОМВ – сучасні високі соціально-гуманітарні технології створення, зберігання, розповсюдження та пошуку інформації. До них відноситься SMM, SEO, таргетинг, контекстна реклама, медіа-віруси та ін.

SEO (Search Engine Optimization) – комплекс заходів із пошукової оптимізації, орієнтований на підвищення позиції веб-сайту у пошукових системах.

SMM (Social Media Marketing) – комплекс заходів із просування персонального акаунту або окремого контенту в соціальних мережах.

Таргетинг – рекламний механізм, що дає можливість виокремити з наявної аудиторії лише певну її частину, яка відповідає потрібним критеріям, і показати саме їй рекламне повідомлення.

Контекстна реклама – метод розміщення інформації, що орієнтована на зміст інтернет-ресурсу, представлена у вигляді банеру чи текстового повідомлення.

Медіа-віруси – інформаційні носії (події, скандали, чутки, діяльність організацій та окремих осіб), що несуть в прихованому вигляді завуальовані ідеї та меседжі.

Хай-сенсоро в ІОМВ − сучасні високі психотехнології, що дають можливість регулювати та керувати соціальними комунікаційними процесами на

рівні соціальних груп та окремих індивідуумів. Типовими в цьому аспекті є соціальна психологія, прикладний психоаналіз та НЛП.

Соціальна психологія – галузь в психології, що орієнтована на вивчення принципів та закономірностей діяльності людини в умовах взаємодії в соціальних групах. Основні проблеми соціальної психології: закономірності спілкування та взаємодії людей, діяльність великих (нації, класи) і малих соціальних груп, соціалізація особистості та розвиток соціальних установок.

Прикладний психоаналіз – напрямок знань в психології, що досліджує практику використання ідей та концепцій, орієнтованих на досягнення глибокого розуміння різноманітних аспектів людської природи, культури та суспільства. Найбільша кількість досліджень в цьому плані припадає на галузі історії, біографії, літератури, мистецтва, релігії, міфології та антропології.

Нейро-лінгвістичне програмування – технологія моделювання вербальної та невербальної поведінки людей за допомогою поєднання форм мовлення, руху очей, тіла та пам'яті.

У структурі зазначеної моделі існують елементи, що мають ознаки двох аспектів. Це Системи підтримки прийняття управлінський рішень (СППУР) та Системи штучного інтелекту. Вони мають характерні ознаки хай-тек та хай-х'юм.

Кожен з зазначених аспектних напрямків має свої методологічні складові та прикладні інструменти, що в комплексі формують сучасну систему управління інформаційно-комунікаційними процесами, в форматі економічних, політичних, військових, культурних та громадських конфліктів.

Основою будь-якого інформаційного протистояння є **інформаційний процес**, що визначається як діяльність із створення, накопичення, зберігання, пошуку та розповсюдження відомостей або даних певного тематичного характеру.

Базовими поняттями для вивчення сучасних мережевих інформаційних протистоянь є **інформація** та **комунікація**, які формують основу всього того, що в подальшому розглядається як інформаційна війна.

Інформацію розуміють як відомості або дані про навколишнє середовище, що оточує людину. А комунікація − це процес передання або обміну інформацією.

У різні епохи інформаційні процеси носили в собі відбитки тих технологій, які було винайдено на певному етапі. Це позначалося на особливостях проведення відповідних інформаційних протистоянь.

Кожен з таких винаходів за історичною значущістю та технічними характеристиками можна визначити або як **інформаційний вибух,** або як **інформаційну революцію**.

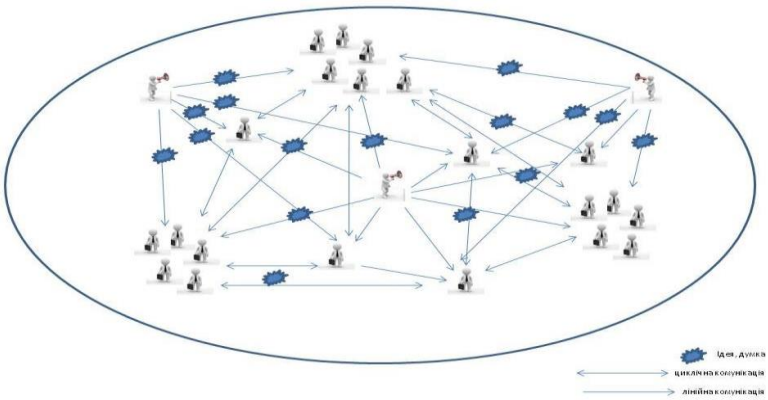
Під поняттям ***інформаційна революція*** ми розуміємо докорінну зміну методів створення, накопичення, зберігання, пошуку та поширення інформації. До таких явищ можна віднести появу мовлення, писемності, комп'ютерної техніки. Всі ці винаходи були початком принципово нового напрямку розвитку інформаційно-комунікаційних технологій.

За визначенням, ***інформаційний вибух*** – це суттєве прискорення процесів створення, накопичення, пошуку та поширення інформації. Типовим прикладом останнього є винайдення абеткової писемності (як модернізація системи писемності), друкарства (оптимізація писемних процесів), Інтернету (еволюція комп'ютерних технологій).

Будь-які інформаційні процеси відбуваються в певних площинах або теренах, які можна узагальнити в рамках поняття **інформаційне поле.** Останнє визначається, як ***соціальний або географічний простір,*** у межах якого відбуваються типові комунікаційні процеси, які охоплюють їх учасників (суб'єкти) на основі обміну інформацією (об'єкт) (мал. 1.35).

Складовими частинами інформаційного поля є **суб'єкти інформаційних процесів**– учасники комунікацій, індивідууми, соціальні групи, організації (ЗМІ, громадські, державні, комерційні структури). Також важливою складовою частиною інформаційного поля є об'єкти інформаційних процесів − інформація або ті, хто отримують цю інформацію в процесі спрямованої комунікації.

Суб'єкти та об'єкти інформаційних процесів поєднуються між собою за допомогою **лінійної** або **діалогової моделей** соціальних комунікативних процесів (мал.15).



Мал.15. **Інформаційне поле**

Лінійна модель комунікації передбачає однобічний, цілеспрямований процес передання інформації від автора повідомлення до отримувача. На першому етапі у свідомості автора з'являється певна ідея (думка) яку він, на другому етапі, перетворює на інформацію шляхом кодування – матеріалізації ідеї у вигляді слова, тексту, малюнка, звука. Сформована таким чином інформація (контент) на третьому етапі транслюється через посередника (технічні засоби комунікації або інша особа) або особисто автором (артикуляція або

демонстрація). На четвертому етапі повідомлення досягає отримувача, який його декодує (читає, переглядає, прослуховує) для того, щоб зрозуміти базову ідею (думку), яка була закладена автором повідомлення. Надіслану ідею отримувач обробляє та формує власне судження з цього приводу у вигляді певної ідеї. На цьому процес лінійної комунікації закінчується.

У разі, якщо отримувач інформації має намір відреагувати на повідомлення, він спрямовую свою думку, на основі отриманої ідеї автору, застосовуючи той же самий механізм. Він кодує свою думку, транслює її, потім відбувається її декодування та сприйняття. Це ***циклічна модель комунікації***, яка передбачає взаємний обмін інформацією, в процесі якого учасники комунікації поступово змінюють ролі автора та отримувача повідомлення (мал. 16)**.**

Мал.16. Базовий комунікаційний процес

Базовими сферами застосування сучасної інформаційної війни є: політична, дипломатична, військова, фінансово-економічна. Інформаційні протистояння в цих сферах, за структурою, виглядають як циклічний або лінійний обмін інформацію, яка може/має спричинити певну шкоду отримувачу, а автору надати певну перевагу. Саме в цьому і полягає сутність **сучасної інформаційної війни.**

Базовою методологічної основою сучасних інформаційних протистоянь є **маніпуляція** − засіб психологічного впливу, що застосовується задля прихованого проникнення в психіку жертв із метою занесення цілей, бажань, намірів, відносин або установок маніпулятора. Фактично, це приховане управління людьми та їх поведінкою.

Головним форматом здійснення інформаційних протистоянь є поняття **інформаційна зброя** або **інформаційна атака.** Останні розуміють як здійснення тимчасового або остаточного виведення з ладу систем та підрозділів противника, що відповідають за процеси управління та інформування.

Головною метою інформаційної атаки є отримання суттєвих переваг в реальному військовому, економічному або політичному протистоянні.

Традиційним базовим інструментом інформаційного протистояння є **медіа**, які здійснюють посередницьку функцію із трансляції ідей та думок у вигляді конкретних меседжів, між автором повідомлення та отримувачем. Медіа розуміють як канали та засоби зберігання, передачі і подання інформації або даних. До медіа можна віднести будь-який інформаційний носій, що виконує означені функції. Разом з тим існує ще таке поняття як **масмедіа**, яке іноді ототожнюють із поняттям медіа. Втім масмедіа мають дещо конкретніші обриси і визначається як: **технології та засоби трансляції** інформації від конкретного джерела на широку аудиторію, яка обмежується рамками певного інформаційного поля в якому ці мас-медіа діють.

Типові масмедіа поділяються на три групи, за специфікою функціонування.

⇒ друкована преса (газети, журнали, бюлетені тощо);
⇒ аудіовізуальні (радіо, телебачення, Інтернет);
⇒ інформаційні служби (агенції, прес-служби, прес-бюро, центри громадських зв'язків тощо);
⇒ рекламно-інформаційні носії (зовнішня реклама, візуальна реклама та ін.);
⇒ засоби маскультури (кіно, театри, концерти та ін.)

За регіональним розповсюдження масмедіа поділяються на:

⇒ транснаціональні (на міждержавному рівні);
⇒ національні (в кордонах певного державного утворення);
⇒ регіональні (окрема територіально-адміністративна зона);
⇒ місцеві (прив'язані до конкретної місцевості–місто, район, село або окрема організація).

Здобутком XX ст. стало народження нового формату інформаційно-комунікаційних протистоянь, який отримав назву **кібервійна**. Останню розуміють як боротьбу сторін на рівні програмного забезпечення шляхом видобування закритої інформації та виведення з ладу програмно-апаратних засобів противника з метою отримання суттєвих переваг у економічних, політичних та військових протистояннях.

Головними діючими особами в такій війні є спеціальні фахівці: **хакери** (ті, що видобувають інформацію) та **кракери** (ті, що псують програмно-апаратні засоби).

У форматі кібервійни визначаються наступні види:

- *вандалізм* – псування інтернет-сторінок, зміна змісту негативними або пропагандистськими матеріалами;
- *пропаганда* – поширення звернень, що закликають до певних дій, або розміщення відповідної інформації на чужих інтернет- майданчиках;

- *збирання інформації* – зламування сторінок приватних осіб або окремих організацій для отримання закритої інформації
- *від втручання в роботу програмно-апаратного забезпечення* – dDoss атаки на комп'ютери, що виконують адміністративно-контрольні функції в державних, громадських, військових та комерційних організаціях;
- *атаки на мережеву інфраструктуру* – напад на комп'ютери, що контролюють життєдіяльність міст, зокрема телефонних ліній, водопостачання, електропостачання, пожежної безпеки, транспортного сполучення та ін.

З народженням інтернет-технологій web 2.0 формується новий напрямок інформаційних конфліктів – **мережева війна**. Це поняття містить таке визначення, як: інформаційно-комунікаційне протистояння у форматі оф- лайн та онлайн мережевих структур.

Типовими **оф-лайн мережевими структурами** вважаються організації або тимчасові/ситуативні об'єднання індивідуумів на основі спільної діяльності або загальних інтересів.

До **онлайн мережевих структур** відносяться **інтернет-ресурси формату WEB 2.0-3.0– віртуальні соціальні мережі** (VKontakte, Facebook та ін.).

Провідне значення в теорії, методології та методиці ведення сучасних інформаційних війн посідає поняття **гібридна війна**. Таку війну розуміють, як: засіб протистояння, який поєднує в собі комплекс різноманітних інструментів політичного, економічного, військового та ідеологічного характеру. Іноді для визначення цього явища застосовують такий термін, як: **асиметрична війна**. Це визначення підкреслює та визначає нетрадиційний специфічний креативний характер протистояння, що відбувається з допомогою нестандартних комбінованих стратегії та тактики ведення конфлікту. Під час такої війни ресурси та характер дій противників відрізняються один від одного. Головна мета – шляхом певної концентрації компенсувати недостатність ресурсів і можливостей однієї із сторін або отримання суттєвої переваги по конкретному напрямку в рамках конфлікту.

Полем застосування інструментів гібридної/асиметричної війни є: населення конфліктної зони, тилове населення, міжнародна спільнота.

Форма ведення такого виду війни:

- громадські заворушення – акції громадської непокори, демонстрації, блокування, вуличні зіткнення;
- повстання – відкритий військовий виступ проти офіційної влади;
- партизанський рух – прихований збройний опір офіційній владі;

- тероризм – організація та здійснення гучних вбивств, підривання транспортних засобів, споруд, місць масових соціальних контактів (онлайн та оф-лайн);
- громадянська війна – військові дії між прихильниками різних ідеологічних, територіальних або національних груп у межах однієї держави.

3. Українське законодавство в галузі інформаційної політики та безпеки

Закон України «Про Державну службу спеціального зв'язку та захисту інформації України». Зазначений нормативно-правовий акт визначає правові основи організації та діяльності Державної служби спеціального зв'язку та захисту інформації в Україні. В Законі встановлюються правила, принципи підготовки повідомлення, зберігання передання інформації, системи доступу до певних типів інформації та умови зберігання пов'язаною з цим державної таємниці.

Закон України «Про державну таємницю». Цей Закон регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України.

Закон України «Про доступ до публічної інформації». Цей Закон визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес.

Закон України «Про електронні документи та електронний документообіг». Цей Закон встановлює основні організаційно-правові засади електронного документообігу та використання електронних документів.

Закон України «Про засади державної мовної політики». Зазначений нормативно-правовийактрегулюєосновимовноїполітикивУкраїні,специфіку та особливості використання української мови як державної та мов національних меншин у територіальномута культурному аспектах.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Цей Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

Закон України «Про захист персональних даних». Зазначений Закон регулює правові відносини, пов'язані із захистом і обробкою персональних

даних, і спрямований на захист основоположних прав та свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних. Поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться в картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів.

Закон України «Про інформацію». Базовими положеннями цього нормативно-правового акту закріплюється право громадян на інформацію, закладаються правові основи інформаційної діяльності. Ґрунтуючись на Декларації про державний суверенітет України та Акті проголошення незалежності, Закон стверджує інформаційний суверенітет України і визначає правові норми міжнародного співробітництва в галузі інформації.

Закон України «Про наукову і науково-технічну експертизу». Закон визначає правові, організаційні і фінансові основи експертної діяльності в науково-технічній сфері, а також загальні основи і принципи регулювання суспільних відносин у галузі організації та проведення наукової та науково-технічної експертизи з метою забезпечення наукового обґрунтування структури і змісту пріоритетних напрямів розвитку науки і техніки, наукових, науково-технічних, соціально-економічних, екологічних програм і проектів, визначення напрямів науково-технічної діяльності, аналізу та оцінки ефективності використання науково-технічного потенціалу, результатів досліджень.

Закон України «Про Національну систему конфіденційного зв'язку». Зазначений нормативно-правовий акт регулює суспільні відносини, пов'язані із створенням, функціонуванням, розвитком та використанням Національної системи конфіденційного зв'язку.

Закон України «Про основи національної безпеки України». Цей Закон відповідно до пункту 17 частини першої статті 92 Конституції України визначає основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності.

Закон України «Про підтвердження відповідності». В Законі визначаються правові та організаційні засади підтвердження відповідності продукції, систем якості, систем управління якістю, систем екологічного управління, персоналу та спрямований на забезпечення єдиної державної технічної політики у сфері підтвердження відповідності.

Закон України «Про радіочастотний ресурс України». Цей Закон встановлює правову основу користування радіочастотним ресурсом України, визначає повноваження держави щодо умов користування радіочастотним

ресурсом України, права, обов'язки і відповідальність органів державної влади, що здійснюють управління і регулювання в цій сфері, та фізичних і юридичних осіб, які користуються та/або мають намір користуватися радіочастотним ресурсом України.

Закон України «Про телекомунікації». Закон встановлює правову основу діяльності в сфері телекомунікацій. Визначає повноваження держави щодо управління та регулювання зазначеної діяльності, а також права, обов'язкита засади відповідальності фізичних та юридичних осіб, які беруть участь у даній діяльності або користуються телекомунікаційними послугами.

Закон України «Про друковані засоби масової інформації (пресу) в Україні». Закон створює правові основи діяльності друкованих засобів масової інформації в Україні, встановлює державні гарантії їх свободи відповідно до Конституції України, Закону України «Про інформацію» та інших актів чинного законодавства і визнаних Україною міжнародно-правових документів.

Закон України «Про телебачення та радіомовлення». Закон регулює діяльність теле-, радіо- організацій на території України, визначає правові, економічні, соціальні, організаційні умови їх функціонування, спрямовані на реалізацію свободи слова, права громадян на отримання повної, достовірної та оперативної інформації, на відкрите і вільне обговорення суспільних питань.

Закон України «Про систему Суспільного телебачення і радіомовлення України». Нормативно-правовий акт, що регулює питання створення та діяльності суспільних засобів масової інформації – телебачення та радіомовлення. Зазначені ЗМІ мають статус незалежних структур, діяльність яких контролюється Громадською радою, до її складу залучаються відомі та незалежні громадські діячі та профільні фахівці.

Закон України «Про інформаційні агентства». Закон регулює порядок реєстрації, формування та практичної діяльності національних інформаційних агенцій та представництв іноземних агенцій. Також визначаються формати та порядок розповсюдження інформаційної продукції в Україні (національна та іноземні агенції) та закордоном (національних агенцій).

Закон України «Про науково-технічну інформацію». Закон визначає основи державної політики в галузі науково-технічної інформації, порядок її формування і реалізації в інтересах науково-технічного, економічного і соціального прогресу. Мета цього нормативно-правового акту - створення в Україні правової бази для одержання та використання науково-технічної інформації.

Закон України «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової

інформації». Закон відповідно до Конституції України визначає порядок всебічного і об'єктивного висвітлення діяльності органів державної влади та органів місцевого самоврядування засобами масової інформації і захисту їх від монопольного впливу органів тієї чи іншої гілки органів державної влади або органів місцевого самоврядування, є складовою частиною законодавства України про інформацію.

Закон України «Про рекламу». Закон визначає засади рекламної діяльності в Україні, регулює відносини, що виникають у процесі виробництва, розповсюдження та споживання реклами. Особливої уваги заслуговує ст. 12, присвячена соціальній рекламі, правилам її використання та тематичному наповненню соціальних інформаційних послань.

Закон України «Про видавничу справу». Закон визначає загальні засади видавничої справи, регулює порядок організації та провадження видавничої діяльності, розповсюдження видавничої продукції, умови взаємовідносин і функціонування суб'єктів видавничої справи. Відповідно до Конституції України цей Закон покликаний сприяти розвитку національної культури, захисту прав та інтересів авторів, видавців, виробників, розповсюджувачів і споживачів видавничої продукції.

Закони України «Про Національну програму інформатизації» та «Про Концепцію Національної програми інформатизації». Закони визначають загальні засади формування, виконання та корегування Національної програми інформатизації. Остання в свою чергу передбачає створення в Україні сучасного інформаційного суспільства, заснованого на організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесах, що спрямовані на створення умов для задоволення інформаційних потреб, реалізації прав громадян і суспільства на основі створення, розвитку, використання інформаційних систем, мереж, ресурсів та інформаційних технологій, створених на основі застосування сучасної обчислюваної та комунікаційної технік.

4. Стратегія та тактика інформаційної війни

Перший рівень – **СТРАТЕГІЯ.** Цей рівень позначає базові напрямки та орієнтири, а також певні умови і характеристики комунікаційних процесів. Перший крок − визначення **мети,** що може висловлюватися в таких варіантах, як:

1. ***Консолідація*** – необхідність сприяння об'єднанню представників цільових груп задля вирішення певних завдань. Така мета може мати місце у ситуації, коли потрібно мобілізувати суспільство в умовах військової агресії,

протидії певним обставинам або силам внутрішнього характеру для вирішення екологічних, соціальних або економічних проблем.

2. ***Консолідація*** – необхідність сприяння об'єднанню представників цільових груп задля вирішення певних завдань. Така мета може мати місце у ситуації, коли потрібно мобілізувати суспільство в умовах військової агресії, протидії певним обставинам або силам внутрішнього характеру для вирішення екологічних, соціальних або економічних проблем.

Практичні приклади

Класичним прикладом ситуації, коли необхідно застосовувати консолідаційний підхід – боротьба із російською агресією (2014-2015 рр.) та (2022- по т.ч.). При цьому слід зазначити, що у випадку з цими подіями консолідаційна стратегія України формувалася переважно стихійно через механізми самоорганізації суспільства, його найбільш активної частини. Громадськість одразу визначила свої пріоритети та висловила їх у соціальних мережах. Замість розгубленості сформувався активний волонтерський рух. Відбулося згуртування навколо традиційних українських цінностей, національна символіка набула шаленої популярності, а гімн став чи не найбільшим хітом. Ініціаторами такого руху в соцмережах стали окремі користувачі та відомі блогери, що дуже швидко об'єдналися у тематичні групи, в яких оперативно обмінювалися інформацією щодо волонтерських справ, розвінчання фейкової та поширення об'єктивної інформації про події на фронті.

3. ***Заспокоєння*** - потреба в зниженні суспільного напруження, агресії, незадоволення представників певних цільових груп або суспільства в цілому. Зазначена мета виникає у разі виникнення внутрішніх несприятливих умов соціально-економічного або політичного розвитку, а також за умови зовнішнього намагання підбурення населення до проявів незадоволення.

Практичні приклади

Унаслідок внутрішньополітичної економічної кризи та зовнішньої агресії протягом 2012-2015 рр. суттєво зросли настрої протесту в українському суспільстві. Цією обставиною дуже активно намагалися скористуватися зовнішні противники, які за алгоритмами гібридної війни створювали штучні кризові ситуації, що призводили до напруження в суспільстві та виникнення громадських протистоянь. Головна теза опонентів – в Україні відбувається громадянська війна. Натомість українське мережеве суспільство інстинктивно, а певні профільні державні структури, громадські об'єднання та окремі блогери цілеспрямовано поширювали матеріали, що вказували на перспективи, створювали позитивний заспокійливий вірусний контент сприяли формуванню національної свідомості та патріотизму, а також актуалізували демократичні цінності з акцентом на європейську інтеграцію.

4. ***Залякування*** – необхідність викликати невпевненість чи острах серед певних соціальних груп, у суспільстві в цілому, по відношенню до певних викликів або загроз. До такого підходу вдаються в разі необхідності припинення розвитку процесів сталого соціально-економічного або політичного розвитку. Це є, в переважній більшості випадків, ознакою прихованої інформаційно-психологічної агресії. Рідше ця мета може мати стримуючий характер або при необхідності дезорієнтації суспільства.

Практичні приклади

Саме таку стратегію – на залякування російськомовного населення Криму та Сходу України перед загрозою націоналістичної агресії з боку політичних організацій «Правий сектор» та «Свобода» застосувала Росія в 2014 р., на початку і впродовж перших етапів агресії. Такий підхід дозволив атакуючій стороні отримати максимально можливу підтримку місцевого населення та формальний привід для введення військового контингенту і надання усіх видів підтримки озброєним бандформуванням, так званих ДНР та ЛНР.

5. ***Невдоволення*** – необхідність виведення із стану рівноваги окремі соціальні групи або суспільство в цілому для формування настроїв протесту. У такому випадку намагаються викликати відчуття дискомфорту щодо існуючих обставин або умов розвитку соціально-економічних чи політичних процесів, стимулюючи громадське невдоволення.

Практичні приклади

Стратегія на викликання незадоволення в суспільстві українською владою впродовж 2014-2015 рр. була головною для сил, які здійснювали інформаційну агресію проти України. Критика рішень влади, поширення інформації про гіперболізовані факти корупції та порушення закону представниками політичної еліти мали на меті формування настроїв протесту в суспільстві та спонукання до реальних акцій громадської непокори.

6. ***Протести*** – публічні дії представників певних соціальних груп або найбільш активної частини суспільства спрямовані проти певних ситуацій, структур або окремих осіб. У такому разі відбуваються дії організовані конкретно або самоорганізовані, внаслідок яких може відбуватися зміна, трансформація або цілковите знищення певних соціальних інститутів, зміна ситуації, усунення певних осіб від керівництва соціально-економічними або політичними процесами.

Практичні приклади

Стратегія орієнтована на підбурення певного контингенту до акцій протесту, громадських заворушень, терористичних актів. Класичним прикладом прояву успішної реалізації такої стратегії є хода 300-ти нацгвардійців військової частини дислокованої в селі Нові Петрівці, на Київщині

13 жовтня 2014 року. Останнє стало наслідком здійснення активної підривної роботи з боку російських спецслужб через соціальні мережі, зокрема через мережу «В Контакті». Через лідерів та найбільш активну частину згаданого підрозділу поширювалися настрої та інформація, що викликала невдоволення військовослужбовців, і, зокрема, була поширена ідея про здійснення ходи протесту.

До першого стратегічного рівня також відноситься другий крок загального алгоритму – **завдання**, які конкретизують та уточнюють шляхи досягнення базової мети. Найбільш типовими завданнями, в рамках SMM-комунікацій, можуть бути наступні:

1. ***Підготовка контенту*** – створення інформаційного повідомлення, що має певну тематичну цільність та цінність. У такому разі контент може бути у вигляді графічного зображення, фото, відео, аудіо або текстового матеріалу, який може бути переданий за допомогою соціальних онлайн мереж.
2. ***Поширення контенту*** – дії спрямовані на якомога широке розповсюдження певної інформації в середовищі конкретних соціальних груп або адресно – на конкретні персоналії.
3. ***Збирання контенту*** – процедура пошуку систематизації та аналізу певної цільової інформації з метою отримання певного бачення ситуації або передбачення певних ситуацій, що можуть мати місце за певних обставин.

Після визначення завдання, наступним логічним кроком є визначення **цільових груп**, по відношенню до яких передбачається вчинення певних комунікаційних дій. Серед них визначаються такі категорії визначення, як:

1. ***Стать*** – соціальна група, що формується за принципом статевої приналежності.
2. ***Вік*** – соціальна група, що формується за принципом вікової приналежності.
3. ***Соціальне положення*** – соціальна група, що об'єднує осіб за подібним соціальним положенням, як то: певний рівень прибутків, рід діяльності, фізіологічні особливості (люди з особливими потребами), расові або етнічні чинники тощо.
4. ***Ситуативні соціальні групи*** – соціальні групи, що формуються за принципом тимчасового об'єднання навколо певної проблеми, ідеї, завдання і не враховують соціальні, вікові та статеві характеристики.
5. ***Персоналії*** – соціальні групи, які формуються з конкретних персон, що викликають зацікавленість у певних комунікаційних ситуаціях.

Четвертим рівнем є характер та зміст **меседжів**, що спрямовуються на визначені на попередньому етапі цільові групи. За своїм характером меседжі можуть:

- ***Закликати*** **–** змушувати, спонукати їх отримувачів до певних дій або рішень.
- ***Констатувати*** – фіксувати певний стан речей, ситуації або факти, що мають місце в певний момент часу.

Другий рівень – **ТАКТИКА**. На цьому рівні визначаються конкретні інструменти та шляхи досягнення головної мети і вирішення завдань (табл. 1). При цьому загальна алгоритмічна послідовність не переривається, а продовжується, зокрема у вигляді п'ятого кроку, який передбачає визначення **каналів комунікацій.**

У випадку роботи із соціальними мережами це, в першу чергу: Facbook, VKontakte, Odnoklassniki, Instagram, Linked In та ін.

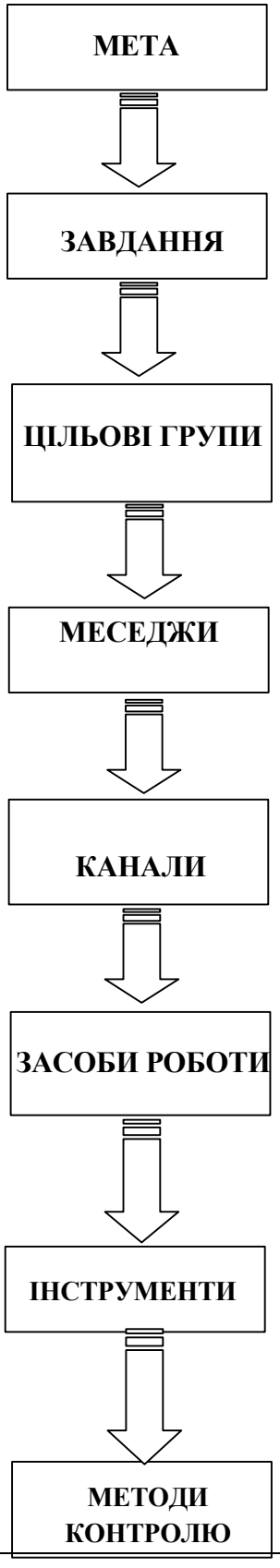
Шостий крок передбачає визначення базових **засобів роботи**, серед останніх:

1. ***Робота на чужих майданчиках*** – розміщення власного контенту або збирання необхідної інформації на чужих інформаційних майданчиках. Такий підхід застосовується у разі, коли необхідно приховати джерело розповсюдження контенту або непомітно для об'єкта дослідження отримати корисну інформацію. Іноді розповсюдження контенту на чужих майданчиках здійснюється із зазначенням адресата – так званий «партизанський маркетинг».
2. ***Робота на власних майданчиках*** – розміщення власного контенту та залучення до співпраці певної цільової групи або персоналій на власних інтернет-ресурсах. У такому разі в певних соціальних мережах створюються тематичні інформаційні майданчики (сторінки, групи, акаунти, події та ін.) відповідно до інтересів, потреб та запитів цільових груп або окремих персоналій, увагу яких необхідно привернути.
3. ***Поєднання роботи на своїх та чужих майданчиках*** – комплексне суміщення роботи на власних та чужих майданчиках, що передбачає проведення складних комунікаційних кампаній, орієнтованих на широке коло цільових груп та персоналій.

Сьомий крок – визначення найбільш типових базових інструментів комунікаційної діяльності у Web 2.0-3.0.

Табл. 1. Базовий алгоритм планування в SMM

СТРАТЕГІЯ	
	- консолідувати - заспокоїти - налякати - викликати невдоволення/гнів - закликати до протесту
	- створити контент - поширити контент - зібрати контент
	- стать - вік - соціальна страта - ситуативне об’єднання - персоналії
	- закликати - констатувати
ТАКТИКА	
	- Facbook - VKontakte - Odnoklassniki - Instagram - LinkedIn - Ін.
	- На чужих майданчиках - На власних майданчиках - Симбіоз власні/чужі
	- Створення та промоція співтовариств бренду - Промоція унишевих соціальних мережах - Створення та розвиток власних інформаційних майданчиків - Промоція контенту - Промоція інтерактивних акцій - Створення та промоція інтерактивних елементів - Робота з лідерами думок - Вірусний маркетинг - Персональний брендинг - Інструменти без категорій - Комунікативна активність - Рейтинги та ТОПи
	- моніторинг - SMM-аудит - опитування



5. Ідеологічні аспекти та психологія сучасної інформаційної онлайн мережевої війни

Базовою складовою частиною процесів інформаційних протистоянь є ідеологія, яка втілюється у вигляді певних меседжів і реалізується за допомогою прикладних методів агітації та пропаганди.

Для успішної реалізації коротких та довготривалих планів у рамках інформаційної війни важливе значення має системність формування ідеологічних складових. Інакше кажучи, потрібно розробити чітку ієрархію в ідеологічному контексті, яка буде складатися із **місії**, **візії** та ситуаційних ідеологічних установок.

При цьому ***місію*** розуміють ***як головну мету, в якій закладається сенс існування та соціальної активності конкретного об'єкта або суб'єкта комунікації.*** Вона є одним з складових елементів стратегічного управління. Саме на основі місії визначається стратегія та позначаються базові основи інформаційно-комунікаційних процесів, що мають застосовуватися в рамках роботи. Місія орієнтується на чітко визначені цільові групи та враховує характери та специфіку інформаційного поля, в межах якого вона буде діяти.

Конкретизація місії здійснюється у вигляді візії або головних завдань, які стоять перед комунікаторомабо комунікантом. У такому разі візія визначається ***як добірка ідеологічних орієнтирів та напрямків комунікаційних процесів, які використовуються для досягнення мети, сформульованої у місії.***

Вже на основі місії та візії розробляється система оперативних ідеологічних постулатів, що складається з базового меседжа (адаптований варіант місії) та тематичних меседжів (візія, головні завдання).

При цьому в плані управління меседжами встановлюється певна чітка ієрархія. Головний меседж несе в собі ключовий інформаційний посил, який розкривається тематично або в розрізі конкретних цільових груп. У такому разі спрямованість меседжів на цільові групи або на теми є ситуативним рішенням, яке залежить від певної комунікаційної ситуації, або конкретних завдань, які необхідно виконати.

Під час розроблення відповідних агітаційних матеріалів активно використовуються зрозумілі для цільової аудиторії образи, символи, цінності, що виступають в якості обгортки, під якою подаються головні меседжі. При підготовці до здійснення прихованої інформаційної атаки до зазначених дій додається ще завдання із маскування цих меседжів.

Для того, щоб ідеї, образи, інформаційні посили чітко відпрацьовували на досягнення поставлених завдань, необхідно враховувати специфіку та особливості соціально-психологічного портрету цільових груп.

Важливим чинником успіху роботи із цільовими групами є відповідь на ключові питання, які дадуть можливість скласти відповідні характеристики:

- Які конкретно соціальні групи є важливими для реалізації завдань (розставити за рівнем пріоритетності)?
- Яким є типовий портрет представника конкретної цільової групи?
- Які уподобання мають представники конкретних цільових груп?
- Яка мотивація спрацьовує по відношенню до представників конкретних цільових груп?
- Хто є безумовними або відносними (по ситуації) авторитетами для представників конкретних цільових груп?
- Які образи, символи, аудіо-візуальні інструменти будуть дієвими в роботі з конкретними цільовими групами?
- Де і на яких комунікаційних майданчиках можна знайти представників конкретних цільових груп (портали, сайти, блоги, соцмережі та ін.)?

Відпрацювавши зазначені питання із комплексної ідентифікації цільових груп та їх представників, можна переходити до вибору символів та образів (свідомі та підсвідомі), що стане основою для відповідного контенту та характеру інформаційних повідомлень. У подальшому до процесу роботи підключають специфічні психотехнології.

Чітке формулювання ідей, меседжів та кодування їх у відповідному форматі (текст, відео, графіка, фото) стає вістрям, своєрідним проникаючим елементом інформаційного тарану, який б’є по свідомості конкретних цільових груп. У цьому контексті важливим компонентом є психологічні методики програмування, маніпулювання та блокування людської свідомості, серед яких особливе місце посідають такі, як? наприклад, **бойове НЛП**.

НЛП визначається як **техніка моделювання** вербальної та невербальної поведінки людей з допомогою поєднання форм мовлення, руху очей, тіла та пам’яті. Відповідно бойове НЛП застосовує ці методи з метою нанесення максимальної шкоди протилежній стороні.

З точки зору теорії і практики НЛП базовим інструментом в досліджуваній темі є **інформаційна зброя**. Останню визначають, як сукупність засобів, методів, способів та технологій інформаційно-психологічного впливу, спеціально створених для прихованого та явного управління інформаційним середовищем противника, процесами й системами, що функціонують на основі інформації, а також для нанесення їм невиправної шкоди.

Основним управлінським процесом визначається **інформаційний вплив**– цілеспрямоване виробництво і розповсюдження спеціальної інформації, яка здійснює безпосередній вплив (позитивний чи негативний) на функціонування та розвиток інформаційно-психологічного середовища держави, психіку та поведінку політичної еліти, населення.

На думку профільних фахівців, у форматі інформаційної війни, в тому числі формату web 2.0, можуть бути застосовані такі технології НЛП, як:

- якоріння, мета моделювання (відновлення мапи реальності);
- субмодальності (перефарбування дійсності);
- шкалювання (порівняння по принципу «більше-менше», «занадто замало»);
- структуризація результату (хто, що, куди, як);
- переривання ланцюга громадської думки (техніка «замаху» та спіндокторінг);
- подолання/створення фобій;
- вирішення/актуалізація інформаційного конфлікту;
- створення майбутнього (ймовірного та неймовірного);
- внесення змін у минуле (пам'ять про небувальщину);
- реімпринтинг формату (пере форматування минулих травм);
- перекодування міфів (швидка зміна переконань);
- побудова системи цінностей (ідеологічне щеплення та перекодування);
- подолання/створення внутрішнього конфлікту.

Особливе місце в практиці бойового НЛП відводиться технологіям гіпнотичного характеру, тобто таким, що впливають на підсвідомість і мають більш серйозні наслідки ніж звичайні форми агітації та пропаганди.

За своєю сутністю, **гіпнотичні методи** – технології зміни стану свідомості, що поєднують у собі ознаки одночасно неспання, сну і сну із сновидіннями. Гіпнотичний транс дозволяє співіснувати одночасно взаємовиключним станам свідомості.

Для здійснення масового гіпнотичного трансу традиційно застосовуються ритмізовані дії, світлові та шумові ефекти, колективне співання. Це можуть бути масові театралізовані заходи, мітинги, масштабні ходи, народні віче тощо.

Застосування таких технологій в інтернет-просторі дає можливість масового трансу фактично у планетарних масштабах, не кажучи про те, наскільки легко таким чином охоплювати окремі країни чи території.

Наслідком застосування таких методів є спалахування серед широких мас населення стану **масового психозу**. Останній визначається як своєрідна психічна епідемія, в основі якої лежать наслідування та навіювання.

Масовий психоз вражає соціальні групи або ситуативно сформований натовп. Унаслідок цього люди втрачають свідому можливість і здатність до раціонального мислення та нормального оцінювання ситуації. Це робить людину одержимою і керованою з боку того, хто застосовує зазначені методи.

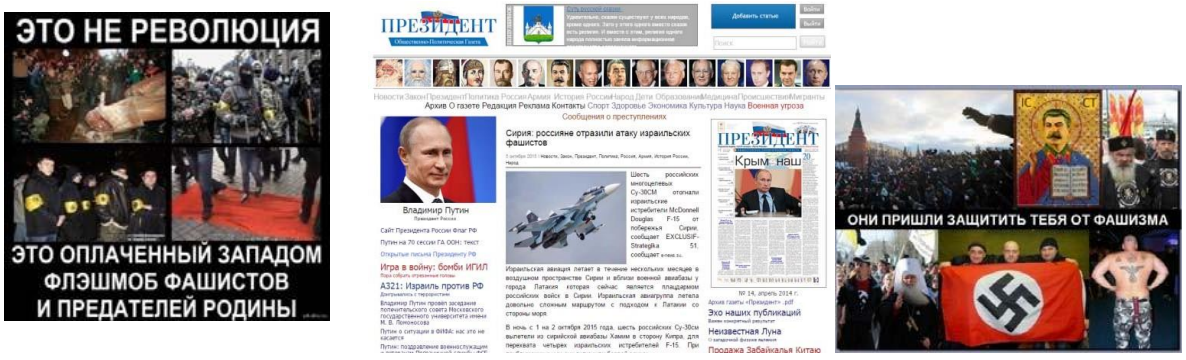
Важливою складовою частиною роботи із масової підсвідомістю є таке явище, як **троп**– риторичний образ, слово або вислів, що використовується у переносному значенні з метою підсилення контенту. Тропи активно використовуються у літературних творах, публічних виступах, повсякденному спілкуванні, в матеріалах ЗМІ. Основними різновидами троп є:*метафора, метонімія, синекдоха, фразеологізм, гіпербола, дисфемізм, каламбур, літота, порівняння, перифразування, алегорія, уособлення, іронія, пафос, сарказм, евфемізм, мейозис*.

Приміром, для сучасної росії такими тропами є «ведмідь», «орда», «руський мир». В Україні до традиційних троп можна віднести такі речі, як «козак», «воля», «Дніпро». Нещодавно для нас цей список розширився за рахунок таких, як «Майдан», «АТО/ООС», «Правий Сектор», «Країна-агресор», «Повномасштабна війна», «Біженці», «Волонтерство».

При застосуванні у соціальних мережах такі тропи вставляються у тексти та іноді використовуються у вигляді хештегів. Найбільш популярними хештегами, в рамках україно-російської інформаційної війни, сьогодні стали такі, як: **#КрымНаш**, **#НяшМяш**, **#ВизиткаЯроша, #RussiaInvadedUkraine, #Снегири, #Двараба, #РаспятыйМальчик** тощо.

Найбільш активно зазначені вище технології застосовують сьогодні в полі діяльності **пропаганди**. Професійна пропаганда, в форматі інформаційної війни, може бути визначена як практика застосування спеціальних форматів, видів, засобів, каналів та технологій соціально-психологічного впливу для перебудови чи укріплення існуючої системи суспільно- політичних поглядів, світогляду людей**.** Серед основних методів пропагандистської роботи визначають:

Навішування ярликів (Name-calling) − застосування при згадуванні противника негативних епітетів («фашисти», «карателі», «нацисти», «кати»).



Мал. 18. **Пропагандистські ярлики**

Узагальнення (Glittering generalities) – асоціювання інформаційного повідомлення із певними типовими цінностями. Зазначені цінності мають бути універсальними та актуальними для різноманітних соціальних груп. В якості прикладу можна розглянути той факт, що путінські ЗМІ подають інформацію проте, що російські бойовики в Донбасі – це інтернаціоналісти, захисники «русского мира» тощо).

Мал. 19. **Узагальнення в агітаційному процесі**

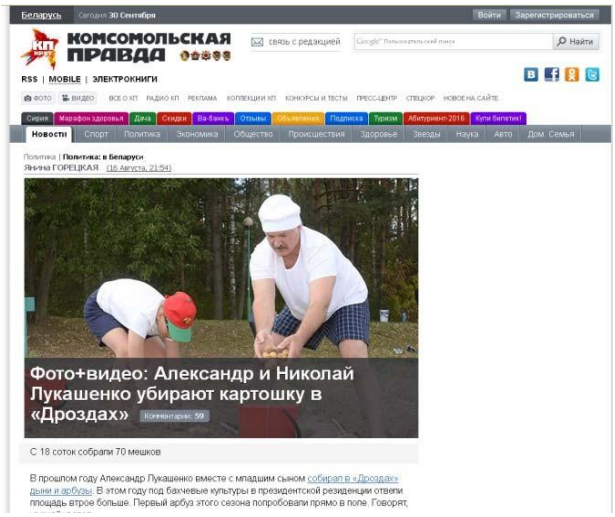
Перенесення (Transfer device) – позиціонування власного повідомлення на фоні широко відомої події, явища, особи. У такому разі розбудовується чіткий асоціативний ряд, який дозволяє автор повідомлення посилювати власні позиції та меседжі, паразитуючи на більш відомих достовірних або історичних явищах. Класичний приклад такої технології меседжі-слогани типу: «діди перемогли фашистів, ми переможемо націоналістів» та ін.

Мал. 20

Засвідчення (Testimonial) – посилання на думку, свідоцтво або коментарі особи, що є лідером громадської думки для певних цільових аудиторій. Таким чином, інформаційне повідомлення паразитує на іміджі конкретної особи. При цьому маємо зазначити, що доволі часто позиція або думка такої особи є рейкова.

Мал. 21. **Метод засвідчення**

Вирівнювання (Plain folks) – представлення лідерів у розрізі звичайних понять, «він з народу», «він читає такі ж газети, як і ми», «він працює на городі» та ін. Останній прийом доволі активно використовується в країнах із напівдемократичними режимами, де певний політичний лідер ще не отримав статус недоторканого і має завойовувати прихильність електорату кожного разу під час перевиборів.

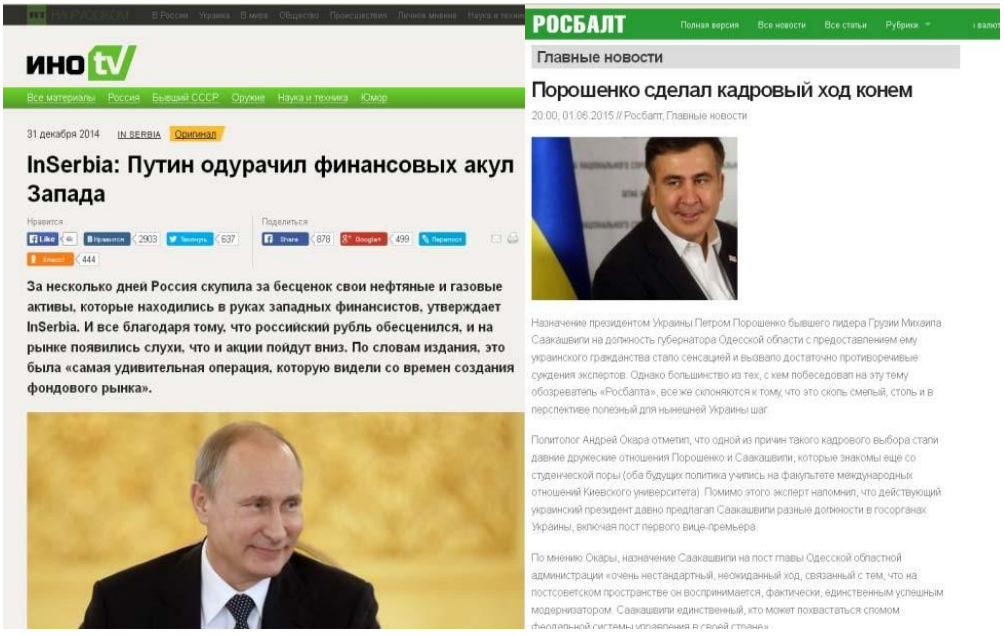


Мал. 22. **Метод вирівнювання**

Як варіант цього прийому існує практика підвищення статусу лідера та перетворення його у супергерої. У такому разі образи керманичів у ЗМІ подаються у вигляді пілотів, мисливців, міцних чоловіків, розумних керівників та ін.

Мал. 23. **Метод підвищення**

Несподіванка (Card stacking) – використання фактів, символів та образів, що є несподіванкою для певної ситуації або цільових груп. Такий прийом є характерною ознакою інформаційно-психологічної війни другого покоління та відноситься до категорії асиметричних дій. Доволі часто такі несподіванки будуються на алогічних рішеннях та діях.



Мал. 24. **Застосування несподіваних повідомлень**

«Заскакування на воза» (Bandwagon) – апеляція або звернення до думки загальної маси, поглядів та переконань широких верств суспільства. Такий прийом є класичною ознакою інформаційної війни другого покоління і реалізується на принципах симулякрів – гри в демократичний процес або його імітацію. Він застосовується для виправдання певних дій та рішень представників політичних еліт або керівництва держави, трактуючи їх як реалізацію народного волевиявлення. Таким було обґрунтування кремлівською владою рішення про анексію Криму, надання допомоги фейковим республікам «ДНР» та «ЛНР» або виправдання СВО.

Висміювання – висвітлення в комічному аспекті національних лідерів або певних історичних подій, що є знаковими для противника. В основі цього прийому лежить принцип висміювання проблеми, що призводить або до нівелювання загрози або до приниження противника. Таким чином, реалізується класичний принцип – те, що комічне, не лякає. Саме за таким принципом формувалась протягом 2014-2022 рр. система інформаційного захисту в соціальних онлайн мережах в Україні проти російської агресії.

Мал. 25. Висміювання національного лідера

Практичний приклад

Класичним прикладом ефективності використання таких технологій є результат застосування росією інформаційно-психологічних методів для обробки населення Півдня та Сходу України з метою забезпечення умов для здійснення результативної військово-політичної агресії та захоплення зазначених територій.

Фактично інформаційно-психологічна війна росії проти України на Сході та Півдні нашої країни розпочалася з перших днів незалежності. То затихаючи, то активізуючись, вона безсистемно продовжувалася фактично до серпня 2008

р. (п'ятиденна війна в Грузії). Саме з цього моменту починається комплексна, системна підготовка до майбутньої агресії з розробкою конкретних кроків, створення відповідних організаційних структур.

Одним з ключових напрямків роботи, яка здійснювалася російською стороною, є закладання певних психологічних установок, активізація яких мала привести до соціального вибуху, в межах певних територіальних груп. Серед таких установок були:

- *захист права на використання російської мови;*
- *загроза українського національного радикалізму;*
- *нерозривність культурних зв'язків з росією;*
- *економічна необхідність співпраці з росією;*
- *зазіхання країн ЄС та США на цілісність України.*

Згідно із попереднім задумом, після досягнення необхідного психологічного ефекту (впровадження установок), у потрібний час, передбачалася активація закладених «психологічних мін» шляхом запуску в ЗМІ та на рівні чуток певних тем. Останнє викликає суспільний резонанс та спонукає до певних дій, на які розраховує атакуюча сторона.

Зазначені установки протягом багатьох років закладалися на свідомому та підсвідомому рівня х у мешканців Сходу та Півдня України, за допомогою всього спектру інструментів інформаційного впливу (ЗМІ, література, кіно, неформальні комунікації та ін.). У 2004 р. пройшла перша обкатка та випробування – ініціювання створення так званої Південно-Східної Української автономної республіки (Донецька та Луганська обл.) та території самоврядування «Новороссийский край» (Одесская обл.).Тоді довести до завершення атаку не вдалося через певну неготовність російської сторони та недостатню глибину ситуації протесту. В 2014 р. готовність російської сторони була більш високою, а ситуація більш сприятливою для розв'язання повномасштабної інформаційно-психологічної.

6. Ситуативне планування інформаційних онлайн процесів

Для систематизації та оптимізації процесів створення і поширення інформації в форматі віртуальних інформаційно-психологічних конфліктів, найбільш ефективним засобом є стандартизація інформаційно-комунікаційних процесів шляхом **алгоритмізації** процедур прийняття відповідних рішень та їх реалізації.

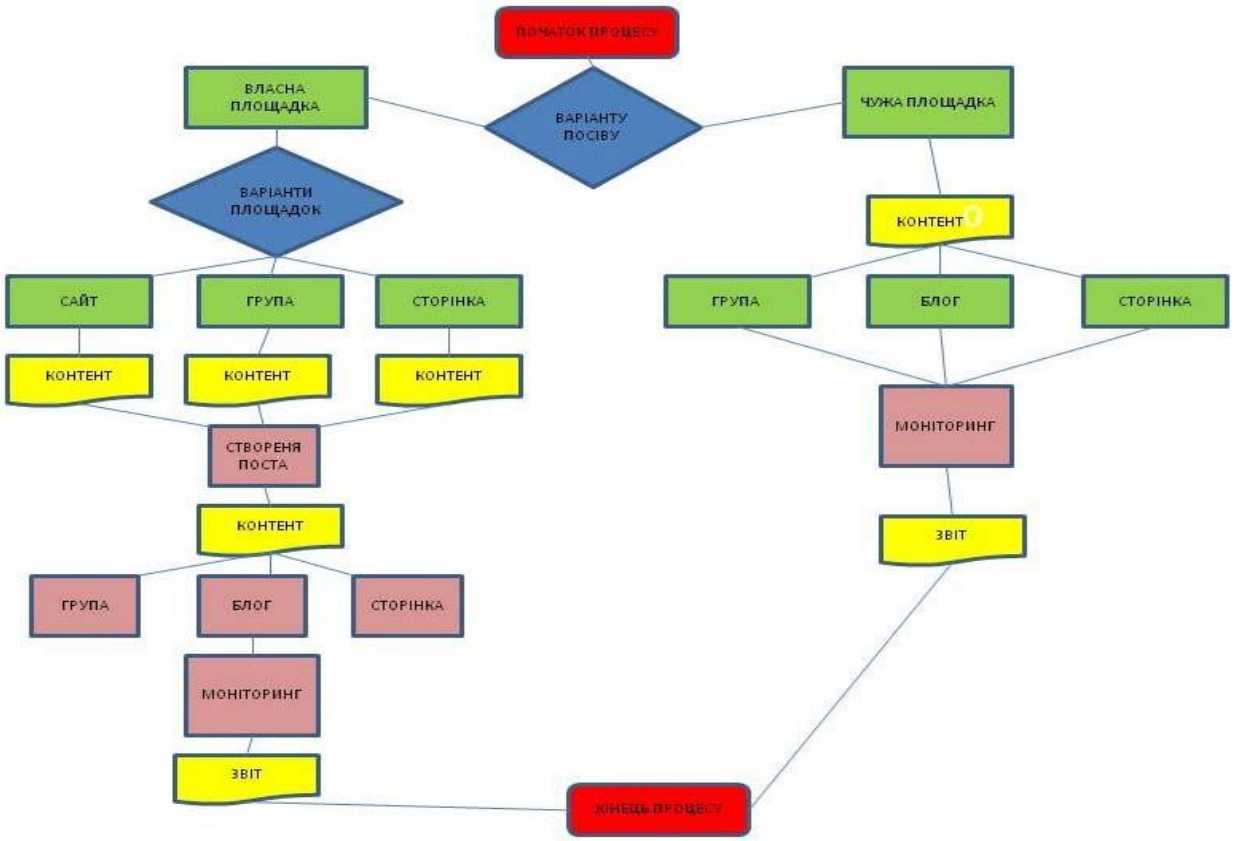
Базовим алгоритмом у такому разі може бути схема, що складається з двох варіантів рішень та відповідних до них етапів реалізації (мал. 26).

Перший варіант рішення – обрання варіанта поширення контенту з власного майданчика. В такому разі контент розміщується на власному сайті, в групі або на сторінці у соціальній мережі, де автор є модератором. Розміщений на такому майданчику контент складає основу для постів, що потім розміщуються вже на чужих площадках – групах (пост або в коментарях), блогах (у коментарях), сторінках (пост або в коментарях). Після розміщення зазначеного контенту здійснюється моніторинг результатів та складається звіт.

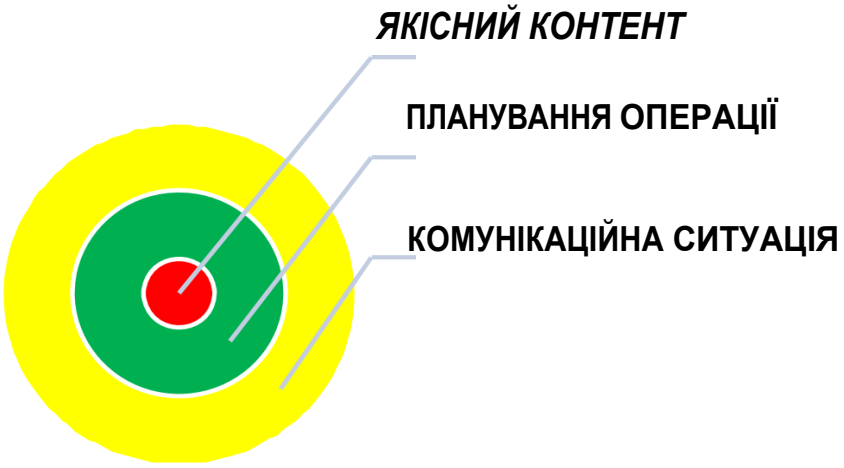
Другий варіант рішення – передбачений для поширення контент розміщується одного разу на чужих майданчиках. У такому разі, це в групах (пост або в коментарях), блогах (в коментарях), сторінках (пост або в коментарях). Після розміщення зазначеного контенту здійснюється моніторинг результатів та складається звіт.

Зазначена схема в цілому спрощена і розкривається у подальшому в конкретних рішеннях та кроках.

Головними складовими частинами успішної інформаційної операції або кампанії є: **комунікаційна ситуація**, **планування** та **контент**.



Мал. 26. **Базовий алгоритм поширення контенту**



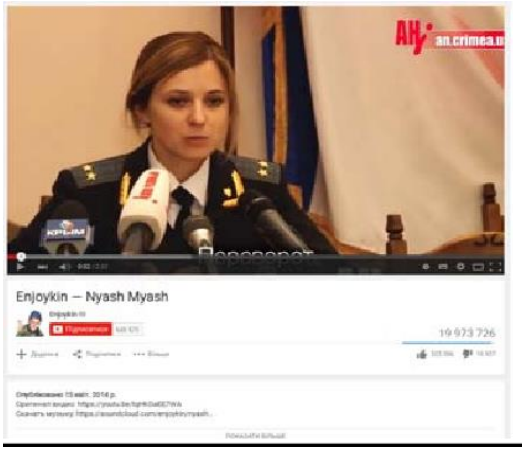
Мал. 27. **Базові умови інформаційної операції**

Оцінюючи комунікативну ситуацію, під час планування операції необхідно врахувати такі аспекти:

- інформація має бути актуальною та профільною для цільових груп, на які вона спрямовується;
- інформація має подаватися саме в той час, коли вона отримає максимального поширення, який не погасить інший більш потужний інформаційний привід або подія;
- для спрощення комунікації, інформація має бути викладена зрозумілою для цільових груп мовою (стиль, ключові слова, поняття, образи, символи).

Базовий алгоритм проведення послідовних етапів операції чи планування передбачає **п’ять послідовних етапів.**

Найбільш якісний контент може перетворитися на вірусний, тобто поширюватися самими користувачами соцмереж за рахунок унікальності або цікавості. Головною умовою «вірусності» є емоційна складова, корисність та можливість здивувати (мал. 28). Контент стає вірусним, якщо отримує від кількох десятків до мільйонів «лайків» та репостів.



Мал. 28. **Вірусний контент, приклади**

Необхідно пам’ятати, що додатковими правилами, які забезпечують успіх при створенні інформаційного повідомлення є:

- гумор та сарказм;
- невеликі обсяги тексту (2-3 абзаци);
- простий та зрозумілий стиль повідомлення (мовою цільових груп);
- використання хештегів (#крымнаш, #четамухохлов тощо) та ріплі (@Posttrans,@VolonretTsentrтаін.);
- широке використання інфографіки.

Поширення контенту. Розповсюдження контенту («розшарування» або «посів») здійснюється в режимі ручного постінгу чи за допомогою окремих програм (сервіси автопостінгу).

Постінг у ручному режимі здійснюється шляхом створення постів у тематичних відкритих групах або на акаунтах. У якості прийомів, які не дуже підтримуються, можна використовувати розміщення власного контенту в коментарях під чужим популярним постом або на чужому акаунті, якщо він є відкритим.

Автопостінг поширює контент у межах заданого простору за визначеними параметрами. Найбільш популярними на сьогодні є такі, як:

⇒ BUFFER – дає можливість розміщувати матеріали у Facebook, Twitter, LinkedIn, App.net и Google+ . Разом з тим Bufferє не тільки автопостером, але й аналітичною системою, яка досліджує соціальні медіа.

⇒ HOOTSUITE – програма для роботи з Twitter, ВКонтакте, Facebook, Google+, LinkedIn, Foursquare и WordPress у браузері або на мобільних гаджетах (мал. 2.14). Через Hootsuite можна не тільки читати стрічки у соціальних мережах, але й публікувати контент. У Pro-версії є масовий завантажувач інформації, що дозволяє працювати з кількома постами одночасно.

⇒ BUZZLIKE – система дозволяє розміщувати пости у VKontakte, Facebook та Odnoklassniki. Пости налаштовуються за часовою стрілкою. В сервісі є шаблони – текстові та з медіа файлами.

⇒ TIME2POST – програма дає можливість працювати з VKontakte, Facebook, Twitter та LinkedIn. Ця система вміє імпортувати повідомлення з RSS, а також створювати водяний знак на зображення. В наявності також є масовий завантажувач зображень. Пости можна планувати за часом або в хаотичному порядку.

Моніторинг результатів. За результатами розповсюдження контенту необхідно відстежити результати щодо складання звіту (див. наступний пункт). Також важливою функцією моніторингу є спостерігання за певним акаунтом,

групою, сторінкою або окремим інформаційним полем, що містяться у певних соціальних мережах. В останньому випадку застосовуються спеціалізовані методики та використовуються відповідні сервіси.

Звіт за результатами. Збирання даних щодо результатів поширення контенту та узагальнення їх у форматі звіту є важливою складовою частиною процесу поширення у соціальних онлайн мережах. Формат та зміст таких звітів поки що не стандартизовано, він може мати будь-яку зручну конфігурацію. Головною умовою є подання перш за все кількісних показників. Серед критеріїв оцінювання є:

- ⇒ кількість репостів – скільки разів цей контент розмістили на власних акаунтах інші користувачі;
- ⇒ кількість «лайків» - скільки користувачів висловили своє позитивне відношення до контенту;
- ⇒ кількість коментарів – скільки користувачів та скільки разів долучалися до дискусії або обговорення контенту;
- ⇒ кількість контактів – кількість учасників груп, сторінок та фоловерів, акаунтів, на яких було розміщено контент.

Представлені вище алгоритми є варіативними, бо відповідно до певних комунікаційних ситуацій або особливостей завдань, на які орієнтуються певні інформаційні процеси, вони можуть корегуватися навіть у момент реалізації.

Такий гнучкий підхід дозволяє оперативно реагувати на певні непередбачувані обставини або перешкоди, які виникають у ході процесу. Постійна динаміка та оцінка перспектив подальшого руху з певних точок біфуркації також дозволяє вишукувати найбільш оптимальні шляхи досягнення поставлених цілей.

У форматі інформаційно-психологічної війни, як складової сучасних гібридних конфліктів, зазначена складова визначається як головна ознака асиметричності процесів.

Разом з тим маємо зазначити, що така гнучкість та варіативність стосується розгортання процесів на окремих етапах. Послідовність цих етапів та їх взаємозв’язок є константним явищем і не передбачає змін.

Інформаційні кампанії зазвичай мають одну стратегічну мету та кілька тематичних завдань. Такі операції є тривалими – від кількох тижнів до року і більше та є поліцільовими.

Протягом тривалого часу (ХХ ст.) такі операції носили лінійний характер і здійснювалися від початку до кінця за чітко визначеною схемою, яка була характерною ознакою першого покоління інформаційно-психологічних війн.

Сьогодні, за умови застосування принципів інформаційно-психологічної війни другого покоління, по ходу реалізації операції завдання можуть коригуватися і навіть змінюватися, при цьому мета залишається незмінною. Це надає таким операціям певної асиметричності, гнучкості, непередбачуваності. Фінал кожного етапу операції перетворюється на точку біфуркації, в який розробляється та приймається певне управлінське рішення, яке відповідає певній комунікаційній ситуації та обставинам, що її формують та впливають на її подальший перебіг.

7. Базові прийоми в інформаційних війнах

У цілому слід зазначити, що застосування інформаційної зброї та ефект від її дії може бути подібний до застосування зброї масового знищення. Глобалізація медіа процесів перетворює окремі інформаційно-психологічні акції на події планетарного масштабу. Саме так це було приміром із терористичною атакою Аль-Каїди на вежі Всесвітнього торговельного центру (Нью-Йорк) та будівлю Пентагону (Вашингтон) 11 вересня 2001 р., яку в усьому світі спостерігали навіть у режимі реального часу.

Зважаючи на зазначені вище обставини, проти інформаційної атаки краще всього діяти або **на випередження**, шляхом **оперативного реагування,** або створивши потужний **ментальний бар'єр** у свідомості тих, хто має стати ціллю такої атаки. В усіх трьох випадках основний формат дій – **розвінчання** неправдивої інформації.

Серед засобів захисту від інформаційної атаки найбільш ефективним є **робота на випередження** шляхом поширення у певному інформаційному полі (де станеться атака) інформації, яка може бути інструментом атаки із відповідними поясненнями або застосовуючи сарказм чи гумор. Таким чином, потенційні отримувачі небезпечної інформації – представники конкретної цільової групи або кількох груп будуть готові до прийому такого повідомлення та сприйматимуть його критично.

У цьому разі створюється малий, тимчасовий ментальний бар'єр, що стає свого роду тимчасовим щепленням від інформаційного вірусу, який вкидає супротивник у наше інформаційне середовище.

Практичний приклад

Спрацювавши на випередження, розмістивши відповідні матеріали у власних ЗМІ (преса, інтернет-видання, радіо та телебачення), українській стороні вдалося випередити, в плані інформаційної атаки, провокації з боку терористичних угруповань ДНР-ЛНР. Втративши ефект несподіванки та можливість звинуватити в обстрілах українську сторону, провокатори відмовилися від своїх планів.

Оперативне реагування є антикризовим інструментом ситуативного характеру. Він застосовується в разі, коли інформаційна атака застала атаковану сторону зненацька, а її наслідки не можна ігнорувати через потенційно небезпечні наслідки. В такому разі, через попередньо сформовану інформаційну мережу (ЗМІ, постінг у групах, інформація на акаунтах відомих блогерів) надається інформація спростовуючого та роз'яснювального характеру. У цьому плані результативність захисту напряму залежить від якості обгортки контенту. Особливо цінними у такому разі є вірусні матеріали.

Найбільш результативно в таких випадках працює так зване «сарафанне радіо», яке по ефективності впливу на широкі маси є важливішим іноді за класичні ЗМІ, бо транслюється у неформальному середовищі від знайомих джерел. Саме тому повідомлення в ЗМІ та соціальних мережах потрібно формувати під стандарти чуток – проста форма, зрозумілі ідеї, сенсаційний характер. Для виконання таких завдань краще всього використовувати блоги та мікроблоги, а також підключати відомих блогерів із широкою власною мережею контактів.

Типовими для інформаційної війни в цілому, а також дієвими для інформаційної війни у соціальних онлайн мережах є такі **методи нейтралізації** інформаційних атак, як:

1. **Парасолька** – обмеження технічним шляхом (блокування доступу до окремих порталів, сайтів, соціальних мереж).
2. ***Воронка*** – нейтралізація певного повідомлення шляхом поглинання на фоні великої кількості інших.
3. ***Колесо*** – заміна певного повідомлення іншим, як більш важливим та статусним.
4. ***Заміна*** – спростування певної інформації шляхом викликання недовіри до джерела розповсюдження повідомлення.

Практичний приклад

У період захоплення російськими військами АР Крим в українських ЗМІ з'явилася інформація про те, що через Чонгар у бік Запоріжжя висувається колона російських танків. Інформація спричинила значну паніку в соціальних мережах та призвела до певних негативних наслідків у системі державного та військового управління. Зусиллями блогерів-активістів ця інформація була оперативно перевірена та відповідне спростування було поширено в українській частині онлайн соцмереж.

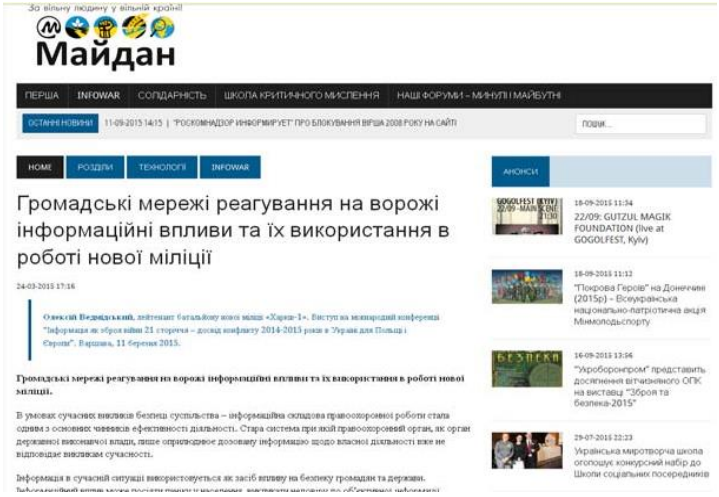
Такий прийом неодноразово використовувався російською стороною з максимально разючим ефектом. Згодом українська сторона навчилась відповідним чином реагувати на такі інформаційні провокації. Зокрема найбільш ефективним засобом стала робота на випередження.

Найбільш надійним засобом боротьби із інформаційними атаками є **створення тотального ментального бар'єру**, який може витримати будь-які несподіванки. При цьому отримувачі інформації будуть знаходитися на певних ідеологічних позиціях, що дозволить їм критично сприймати або взагалі не сприймати шкідливу інформацію. Створення такого механізму є довготривалим процесом та передбачає налагодження системного інформування на основі мультимедійного ефекту та багатократного повторення певних попереджень,

розкриття механізмів можливих маніпуляцій та типових фейків, з якими можуть стикнутися основна маса населення.

Формування такого роду захисту є комплексною роботою, до якої необхідно залучати зусилля та ресурси суспільства, держави та окремих громадських лідерів.

Практичний приклад

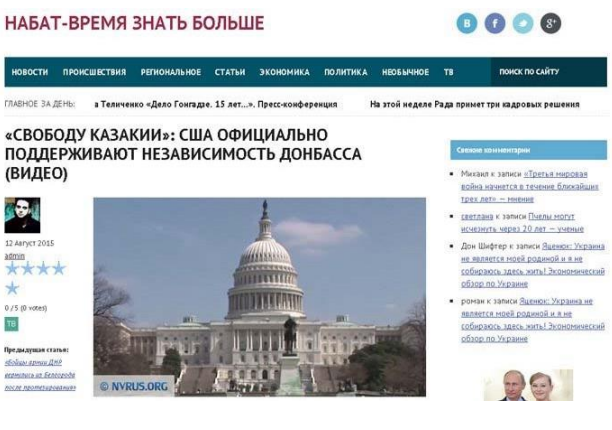


Багато громадських об’єднань та рухів сьогодні займаються просвітницькою роботою, підготовкою певних соціальних груп, потенційно вразливих щодо можливих інформаційних атак.

Найкращим форматом боротьби із інформаційними атаками є **розвінчання фейку** із тлумаченням характеру та реального змісту повідомлення.

Зважаючи на той факт, що переважна більшість інформаційних атак у форматі сьогочасних інформаційно-психологічних війн є анонімними, одним з ключових механізмів розвінчання є з’ясування та доведення до відома широкої громадськості авторів агресії або тих, на чию користь вона працює.

У залежності від характеру та специфіки інформаційної атаки до справи розвінчання необхідно залучати різного роду ресурси. Найбільш ефективними в цьому плані є неформальні або такі, що є авторитетними для відповідних



цільових груп. У разі масштабності нападу до процесу розвінчання мають залучатися всі можливі ресурси – державні, громадські, індивідуальні.

Практичний приклад

Перекрутивши зміст резолюції про «Тиждень поневолених народів» (1956р), російські ЗМІ поширили інформацію про визнання з боку США країни «Казакії» (Донбас, Кубань, Ростовська обл.). Цей фейк було спростовано шляхом надання повного тексту резолюції та відповідних роз'яснень.

Найбільш ефективними прийомами інформаційних атак є: **дезінформація, залякування, схематизм, глузування, вклинювання, фальшування**.

З метою введення противника або цільові групи, що визначені як мішень для атаки, застосовується ***дезінформація – надання хибної інформації***.

Практичний приклад

Перші тижні після перемоги Євромайдану в східних та південних регіонах України поширювалися на рівні місцевих офіційних ЗМІ (преса та інтернет-видання окремих політичних структур) неправдиві повідомлення дискредитуючого характеру. Приміром абсолютно серйозно говорилося про відрахування грошей з зарплат шахтарів та металургів на відновлення Майдану. Останнє окрім політичного подразника (бендерівський Майдан) мало ще й економічний. Ця інформація з часом набула формату медіа-вірусу та через неформальні канали комунікації отримала максимального поширення.

Для відволікання уваги від реальних цілей та намірів противника й представників цільових груп-мішеней частіш за все застосовують ***залякування*** – трансляція інформації, що має на меті порушення рівноваги та формування тривожних або панічних настроїв**.**

Практичний приклад

На початку російської агресії на Сході України та в Криму активно поширювалися повідомлення про те, як українські радикальні націоналістичні організації готуються тероризувати російськомовне населення. Останнє викликало панічні настрої, а під це в свідомість місцевих мешканців закладалися ідеї про необхідність створення загонів самооборони та відокремлення територій від України.

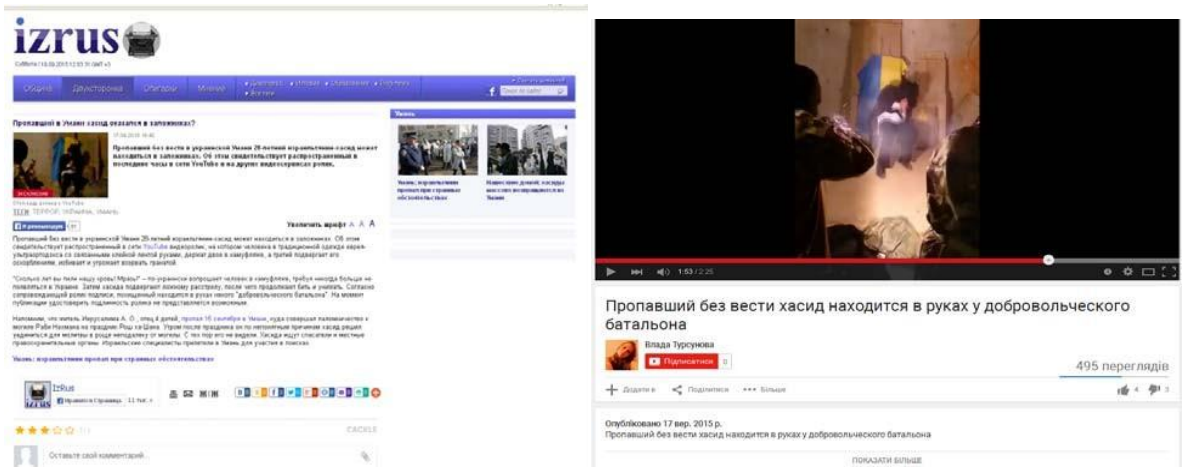
Окрім матеріалів у друкованих ЗМІ та повідомленнях з інтернет-видань було запущено в якості вірусних роликів відео з постановочними кадрами вуличних зіткнень, під час яких молодики з українською націоналістичною символікою підпалюють авто, тероризують пересічних громадян. Особливою популярністю користувалися виступи фейкових свідків злочинів Нацгвардії або бойовиків «Правого сектору», як то: Галини Пишняк про розіп'ятого хлопчика, свідків, що розповідали про винагороду «українським карателям» за участь в АТО у вигляді клаптика землі і двох рабів та інші.

Для спрощення та прискорення сприйняття інформації її отримувачами застосовується ***схематизування*** – графічно-кількісна подача даних у доступному для представників цільової групи форматі. Представлена в такому вигляді інформація використовує принцип образно-символьного сприйняття, яке вважається найбільш ефективним для промоції певних ідей або ідеологічних концепцій.

Під час підготовки до ведення активних дій в офлайн форматі та в якості нейтралізації передбачень щодо потенційних можливостей противника використовують метод **глузування** – виставлення противника та його можливостей в комічному світлі. В такому разі спрацьовує психологічний принцип те, що комічне, не викликає страху або опасінь.

У якості своєрідного інформаційного айкідо для посилення ефективності та атакуючого потенціалу можливо застосувати **вклинювання** − використання інформаційних повідомлень противника шляхом додавання до них певної інформації і корекції повідомлення в потрібному руслі.

Скориставшись повідомленням про зникнення хасіда, що прибув до Умані на святкування нового року, група прибічників росії зняла відео, на якому начебто представники добровольчих батальйонів катують викраденого громадянина Ізраїлю.



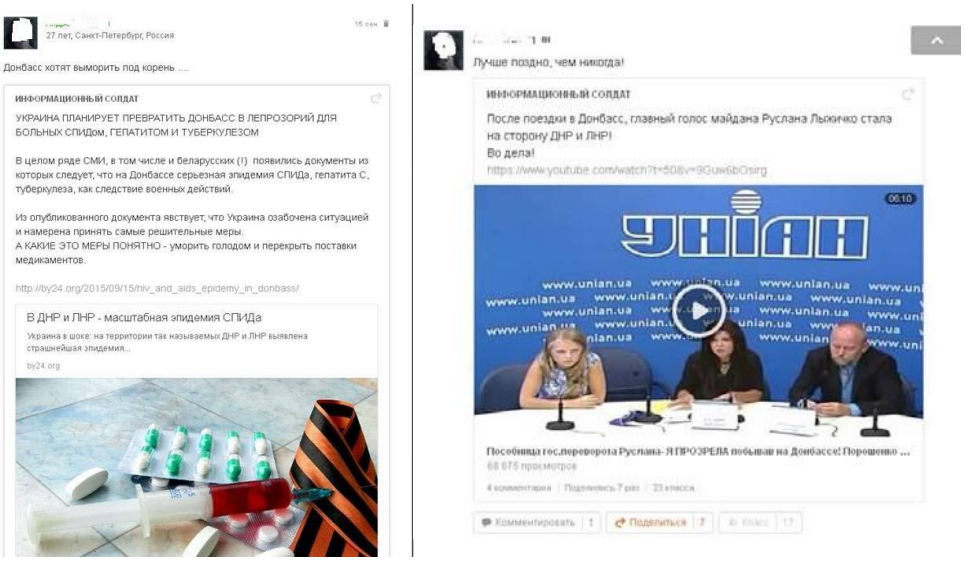
У соціальних мережах цей прийом зазвичай використовують для того, щоб на фоні повідомлення ЗМІ, яке не викликає сумніву, подати приховані меседжі або психологічні установки. Для цього, в якості базової основи для повідомлення, обирається потрібний матеріал (посилання, фото, відео), а на додаток до нього у ліді (анотація або підводка до матеріалу) концентрується те, що є основним змістом. Для загальної маси фоловерів, яка не має критичного сприйняття мережевої інформації, такий прийом є досить результативний.

Практичний приклад

Так, українськими інформаційними бійцями на основі матеріалу білоруського інтернет-видання http://by24.org про масштабну епідемію в ДНР-ЛНР було створено пост, що мав на меті поширення панічних настроїв серед так званих ополченців та місцевого населення, яке підтримує росію.

Також можна навести приклад застосування аналогічного прийому з протилежного боку, коли за основу для атакуючого повідомлення було взято

ролик з емоційним виступом української співачки та громадського діяча Р. Лижичко про ситуацію на окупованих територіях Донбасу. Головна мета мережевого повідомлення в цьому випадку – використання авторитету лідера громадської думки для посилення тези та приховання реальних намірів.

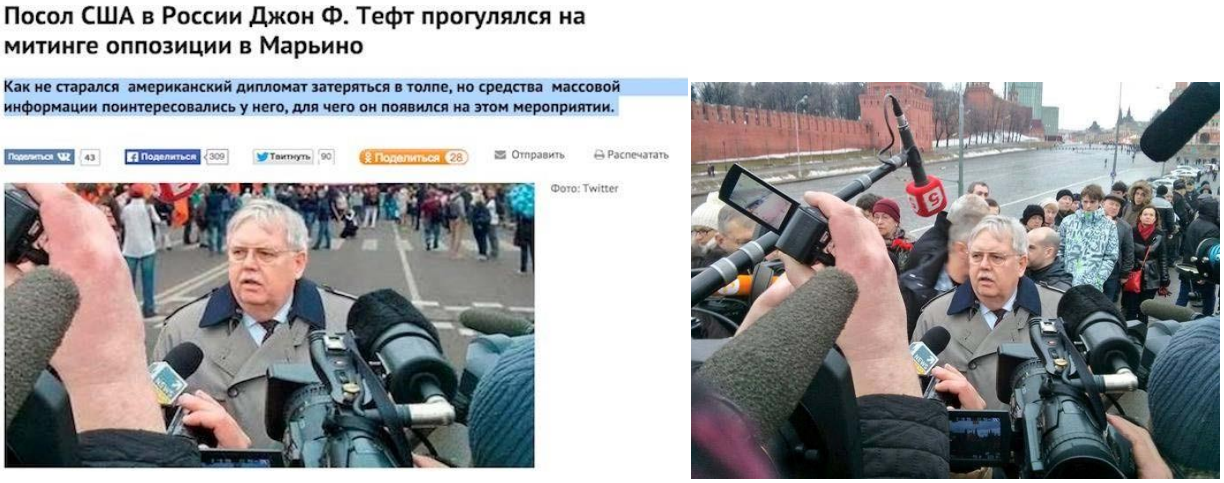


Фактично впродовж усього періоду інформаційної війни, яку веде Росія проти України, через брак візуальних матеріалів використовується контент з іншими подіями, що є **класичним методом фальшування.**

Практичний приклад

Прибічник «ДНР» у своєму блозі видав фото подій в Ізраїлі за події в Донецьку. Представники ЗМІ фейкових республік доволі часто використовують задля ілюстрації власних меседжів спотворені або перекручені матеріали, в тому числі відео для підкріплення власних позицій.

Приклад застосування інтегрованого маніпулювання з позиціонуванням на фоні відомого інформаційного бренду та заголовка-якоря, який гіперболізує зміст самої статті.



Типовий приклад маніпуляції в газеті «Комсомольская правда» (ліве фото). Інформація про те, що посол США начебто відвідав у Москві акцію протесту опозиції, ставши її духовним лідером. Для ілюстрації цієї інформації дали змонтоване фото посла на фоні акції. В реальності це фото зроблене в іншому місці (праве фото.)

Однією з важливих складових частин діяльності в будь-яких військових протистояннях є вміння маскуватися або розкривати замаскованого противника. Це мистецтво особливо актуальне і в протистояннях у соціальних онлайн мережах.

Зважаючи на те, що головним засобом боротьби у соціальних мережах є обмін інформацією та спілкування, успішною буде комунікація між тими, хто має однакові погляди або належить до близьких соціальних груп. Саме тому дуже важливо, щоб майданчик, з якого відбувається трансляція інформаційного послання або персональний акаунт мали відповідний вигляд.

Обкладинка та інше оформлення в групах, на сторінках та акаунтах має відповідати образам та символам, характерним тим групам, на які вони орієнтовані. Аватарки на блогах та акантах повинні виглядати також відповідним чином. Це все аксіома, яка не потребує деталізації та обґрунтування.

Більш складним та специфічним є питання функціонування так званих ботів та тролів – фейкових акаунтів, які застосовуються в якості атакуючих одиниць у класичній війні формату web 2.0 та 3.0. Загально відоме негативне ставлення інтернет-спільноти до таких суб'єктів. Ідентифікація в якості троля автоматично викликає недовіру до трансльованої інформації, робить марними всі зусилля та навіть може допомогти зрозуміти плани противника. Тому, особливо важливо мати навички маскування власних фейкових акаунтів та вміння вираховувати ворожі.

Для надання власним акантам більшої правдивості необхідно:

1. **Обирати реальне ім'я**, яке є типовим для представників відповідних цільових груп.

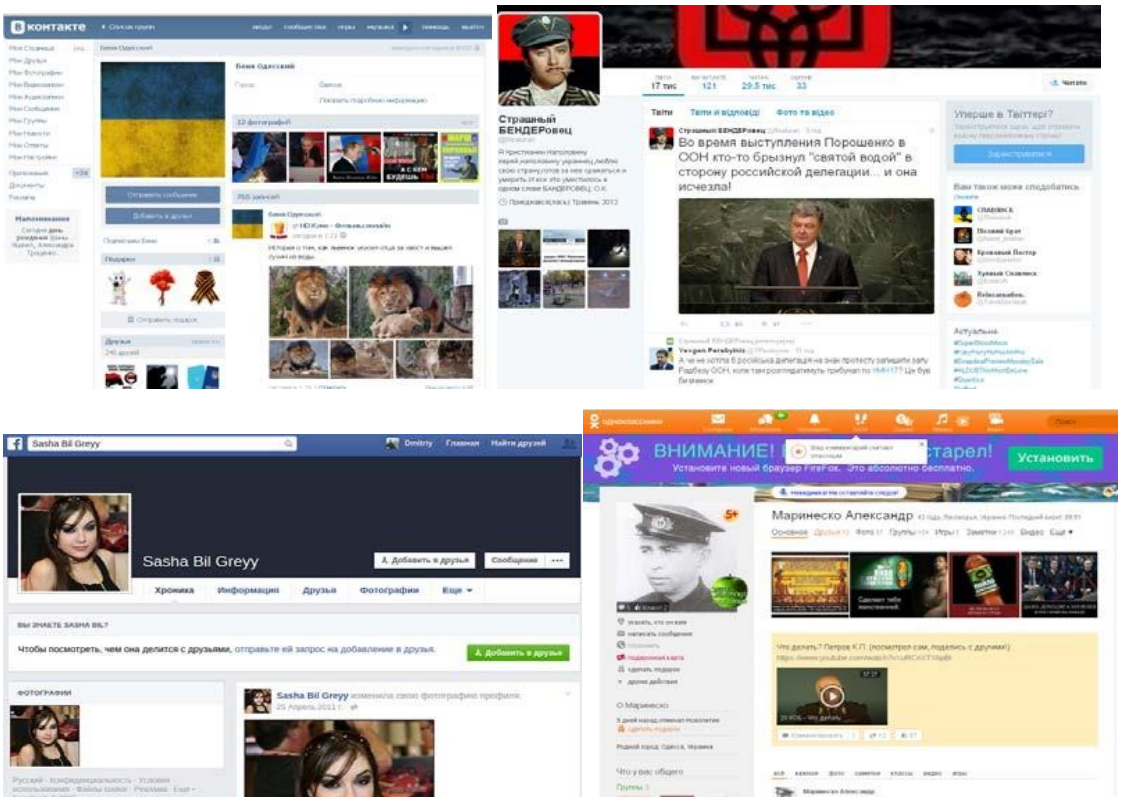
2. **Ставити на аватарку реальне фото** – обирати фотографію будь-якої людини.

3. **Робити акаунт реальним –** створювати персоніфіковані альбоми, підписуватися на різнопланові (не тільки за призначенням троля) сторінки і групи, ставити разом з тематичними пости, що мають розважальний або персональний характер.

Загальне правило – такі акаунти не мають сильно виокремлюватися на фоні інших, вони мають бути типовими, стандартними на фоні відповідних представників цільових груп.

Реєструючи такі акаунти в тематичних групах, необхідно проявляти життєву активність – лайкати чужі пости, ставити нейтральні коментарі.

Життєва активність фейкових акаунтів, крім маскування, має ще одне завдання–налагодження корисних контактів, видобування важливої інформації та вербування прибічників (напряму або «втемну»).



Мал. 29. **Типові фейкові акаунти**

Демаскування фейкових акаунтів, відповідно, відбувається за такими ж трьома ознаками, але в такому разі фіксується їх відсутність або не повна відповідність.

Серед класичних ознак, за якими можна ідентифікувати типового троля, можна визначити такі, як:

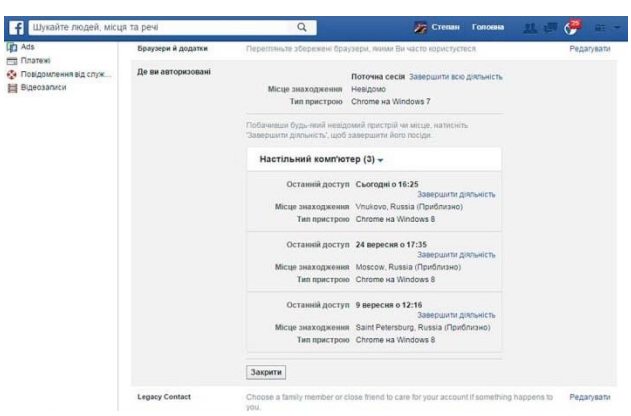
- Шаблонність формулювань та висловлювань, що виникає внаслідок використання кількох варіацій на один меседж;
- Демонстративна лояльність по відношенню до головної теми, занадто палка підтримка офіційної влади, окремих персоналій;
- Висока агресивність, використання ненормативної лексики, персональні образи, знущання, погрози.

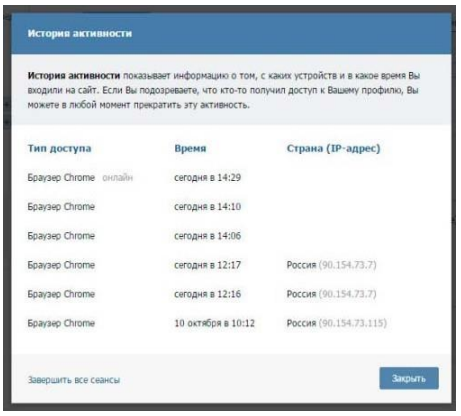
Практичний приклад

Типовим прикладом вдалого маскування та доволі успішного виконання завдань із інформаційно-психологічної диверсії може слугувати діяльність групи, очолюваної мережевим активістом, колишнім бойовиком ДНР Сергієм Жуком, що діяв як медіа-активіст під ніком «Степан Мазур» і позиціонував себе у провідних соціальних мережах під виглядом українського націоналіста.

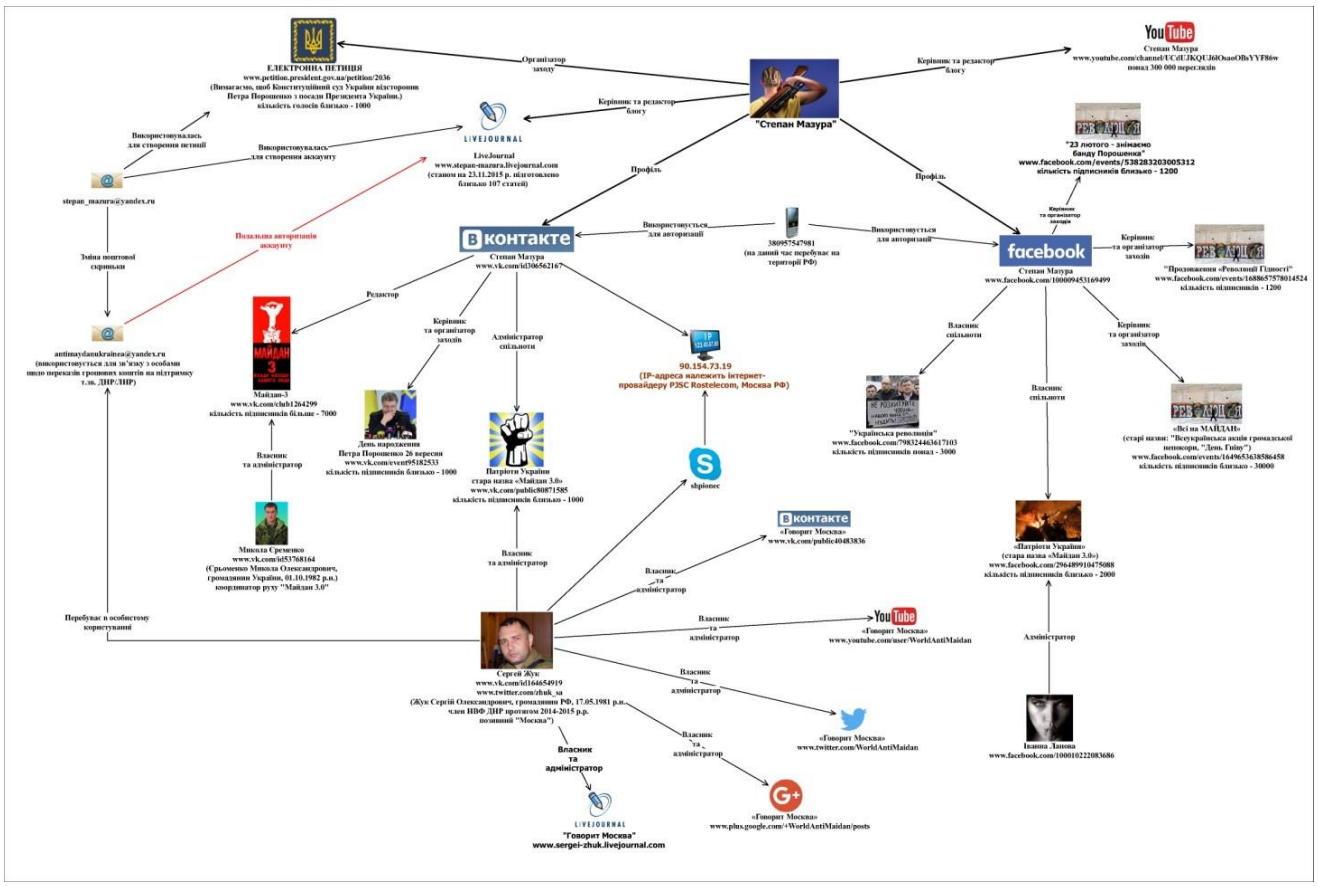
Головним завданням цього агента впливу було підбурення населення проти влади. Для цього було створено групи «Майдан-3» в провідних соціальних мережах. Головним меседжем стали заклики до організації нового Майдану.

«Степана Мазура» доволі швидко вирахували за IP-адресою і встановили місце його базування. Цим місцем виявилася Москва.





Сергій Жук та його команда створили доволі потужну систему, яка протягом певного періоду успішно працювала, виконуючи завдання із здійснення інформаційно-психологічного тиску на користувачів українського сегменту соціальних мереж.



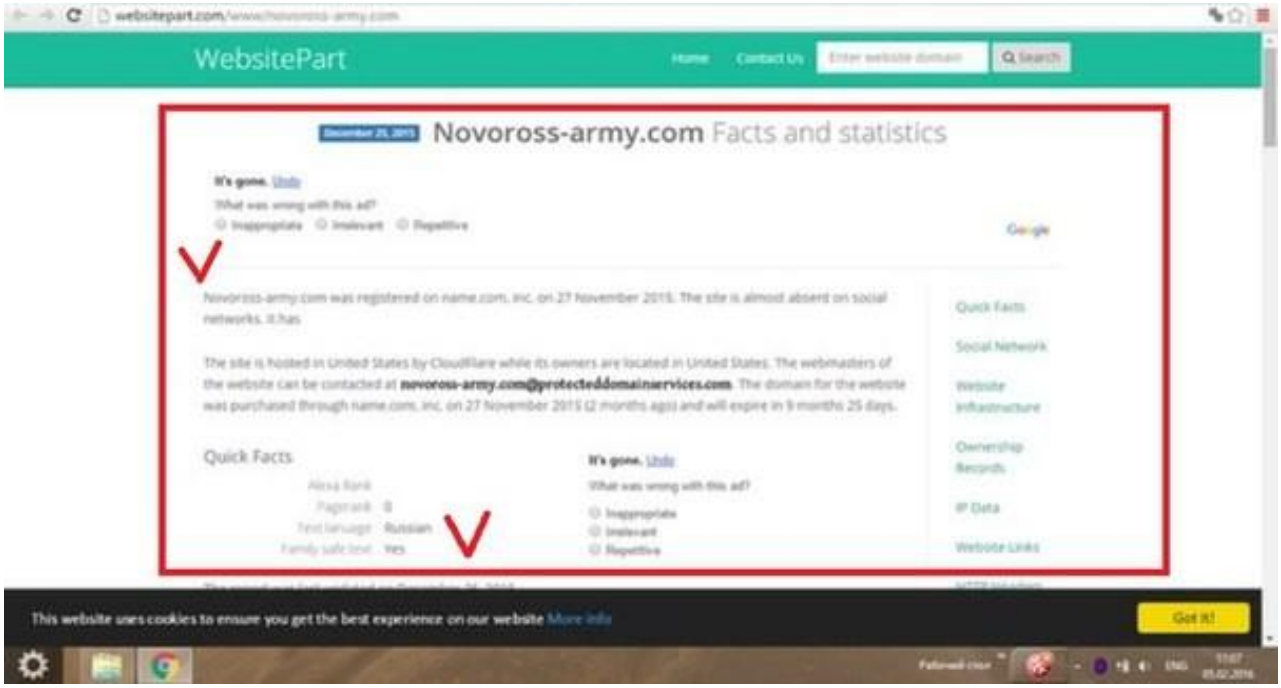
В якості фейкових, добре замаскованих, можуть бути не тільки персональні акаунти, але й окремі інтернет-проекти. В такому разі потрібно буде застосувати більше зусиль та часу для промоції, втім результати можуть бути набагато цікавішими.

Практичний приклад

З метою збирання інформації про учасників незаконних збройних формувань було створено інтернет-портал «Армия Новороссии» (http://novoross-army.com). Проект було створено для «поліпшення комунікації між бійцями та волонтерами, організації збирання адресної допомоги пораненим бійцям…».

Слід зазначити, що автором проекту був 15-ти річний хлопчина, який разом з родиною втік до Львова від окупації з Донецьку.

Адміністратори проекту запевнювали всіх, хто долучався, в тому, що вся інформація шифрується та захищається надійними паролями, а це унеможливлює доступ сторонніх осіб.



Система управління проекту була дуже проста та не вибаглива. А його аргументація та промоція дозволили вже протягом першої години отримати кілька десятків зареєстрованих, які залишили повну інформацію про себе, включаючи контакти.

Сайт пропрацював кілька місяців, генеруючи до 3 Гбайт інформації на день. В цілому вдалось зібрати понад 2,5 тис контактів серед найманців ДНР та ЛНР. І тільки тоді російські фахівці розкрили проект.

Окрім візуальних засобів ідентифікації фейкових акаунтів існує низка технічних інструментів та сервісів, що дають можливість отримувати більш конкретну інформацію:

- знайти сторінку конкретно людини одразу в усіх соцмережах (Yandex);
- знайти останні дописи людини одразу в усіх соцмережах (Facebook, Instagram, Flickr, Tumblr, Vimeo, Reddit);
- дізнатися, що конкретна людина писала на своєму акаунті в конкретний день (Twitter);
- дізнатися тематику та зміст постів мешканців конкретного населеного пункту (Twitter);
- дізнатися, що про конкретну людину пишуть у соцмережах (Social Mention);
- отримати інформацію про нещодавно розміщені та відзняті фотов конкретному місці (Yomapic);
- отримати інформацію про відеоматеріали, в яких фігурує конкретна людина (YouTube);
- ідентифікувати людей на фото (Google);

- визначати, в якому районі придбано сім-карту мобільного зв’язку (gsm-inform.ru);
- вирахувати місцезнаходження через IP (ipfingerprints.com).

Окреме питання, в процесі інформаційної війни web 2.0 – технології пошуку друзів та залучення їх до кола власних інтересів, а також використання на дружній основі чужих ресурсів. Мовою професійної розвідки це називається **вербування** – процес залучення до співпраці на добровільній основі або за певну винагороду (матеріальну чи нематеріальну) персони, яка володіє цінною інформацією або корисними організаційними ресурсами.

Процес вербування в соціальних мережах в основі має класичну схему, але з певною корекцією на специфіку середовища. Зокрема визначаються такі етапи:

1. ***Пошук*** – моніторинг у тематичних групах активних та авторитетних блогерів, що мають максимальну кількість друзів та фоловерів.
2. ***Встановлення первинного контакту*** –лайки під авторськими постами, розміщення улесливих коментарів під авторськими постами, згадування при розміщенні цікавих постів (вказати назву акаунта в статусі та в тексті поста).
3. ***Встановлення дружніх стосунків*** – спілкування в коментарях з поступовим переходом на особисте листування в «лічку».
4. ***Залучення до спільних дій*** – запрошення до власних груп та сторінок, віртуальних заходів або до чатів, створених у «лічку». Як варіант можна надати людині статус модератора у власній групі.
5. ***Стимулювання*** – надання цікавої інформації, корисних посилань, порад за потребою.
6. ***Утримання*** – підтримка постійного інформаційного контакту із цікавим об’єктом, привітання із святами персональними, загальними та професіональними. Звернення за порадами та консультаціями.

Головним полем для роботи із вербування в соцмережах є пости та коментарі під ними у групах, пабліках та на тематичних сторінках.

Базовими засобами, що використовуються при вербуванні, є:

- прояв зацікавленості до конкретної персони та того, чим вона цікавиться;
- «безкорисливе» надання певних власних інформаційних ресурсів;
- промоція об’єкта вербування за рахунок власних ресурсів.

8. Інтернет-реклама та її застосування в інформаційній війні

Реклама, як засіб поширення інформації, може використовуватися не тільки в комерційних цілях, але й як інформаційна зброя при відповідному її застосуванні.

Зокрема за допомогою стандартних рекламних інструментів, типових для багатьох глобальних онлайн соцмереж, можна:

- Пересувати та промотіювати пости та публікації;
- Промотіювати акант або тематичну сторінку;
- Створювати та спрямовувати трафік користувачів на веб-сайт;
- Збільшувати кількість конверсій на веб-сайті;
- Отримувати установки програмних додатків;
- Збільшувати замученість для додатку;
- Промотіювати заходи.

Однією з найважливіших функцій є застосування цільової реклами або, так званий, **таргетинг**. Останній розуміють як рекламний механізм, що дає можливість виокремити з наявної аудиторії лише певну її частину, яка відповідає потрібним критеріям, і показати саме їй рекламне повідомлення.

Виходячи з потенційних можливостей сучасних соціальних онлайнмереж, маємо визначити такі види таргетингу:

1. ***Підбір інформаційно-рекламних майданчиків*** – пошук та використання віртуальних майданчиків (сайти, портали, блоги, групи), на яких рекламодавець може знайти необхідну цільову аудиторію.
2. ***Тематичний таргетинг –*** показ реклами на віртуальних майданчиках (сайти, портали, блоги, групи), що відповідають певній тематиці.
3. ***Таргетинг за інтересами*** – показ реклами у відповідності до інтересів відвідувачів віртуального майданчика (сайти, портали, блоги, групи).
4. ***Геотаргетинг*** – показ реклами за географічним принципом (країна, регіон, місто та ін.) у відповідності до замовлення рекламодавця.
5. ***Гіперлокальний таргетинг*** – показ реклами на всіх пристроях у радіусі від 1 до 15 км від точки трансляції.
6. ***Таргетинг за часом показу*** – демонстрація реклами в певний час дня або день тижня, місяця, року.
7. ***Соціально-демографічний маркетинг*** – показ реклами відповідно до вікових, статевих, соціальних та інших персональних характеристик користувачів.
8. ***Обмеження кількості показів*** – регулювання кількості демонстрації реклами одному користувачеві через банерну рекламу.
9. ***Поведінковий маркетинг*** – збирання інформації про діяльність конкретного користувача з допомогою cookie-файлів – через акаунт користувача (переглянуті сайти, пошукові запити, закупки в інтернет-магазинах та ін.) з метою отримання портрета конкретного представника цільової групи;

10.Геоповедінковий маркетинг – вивчення поведінки та уподобань користувача за допомогою геосервісів у процесі його переміщення.

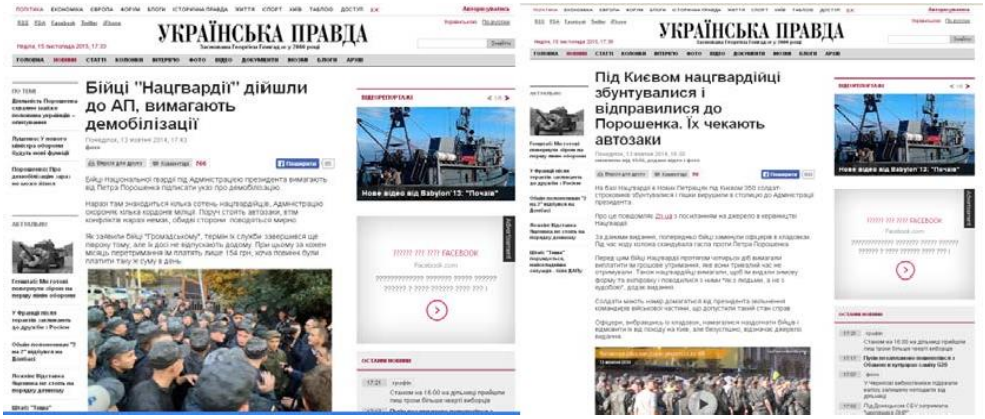
Серед окреслених вище видів таргетингу для здійснення безпосереднього інформаційного контакту із представниками цільових груп, у плані поширення інформації можна застосовувати практично всі. Разом з тим деякі із зазначених інструментів можуть виступати в якості доволі серйозної зброї в рамках не тільки інформаційної, але й реальної війни.

Зокрема, як свідчить практика АТО/ОСС на сході України 20014-2022 рр. та початковий етап широкомасштабного вторгнення (весна-літо 2022р.), російські підрозділи спеціальних операцій широко застосовували гіперлокальний таргетинг, що дозволяло певним чином впливати на психологічний стан українських військовослужбовців, особливо в критичних моментах, коли доступ до об'єктивної інформації був обмежений. Зокрема подавалася інформація, що спонукала до панічних настроїв та капітуляції. Особливо активно такі методи застосовувалися під час боїв за Дебальцево, Київ, Миколаїв, Харків, Сєвєродонецк, Авдіївку, Бахмут.

За допомогою поведінкового та геоповедінкового маркетинга можна здійснювати стеження за певними персоналіями, які є ключовими особами у процесах прийняття та реалізації управлінських рішень. А це вже є фактично виконанням шпигунських функцій стеження. Інші види таргетингу є менш небезпечними, втім не менш дієвими для роботи із конкретними цільовими аудиторіями, стеження за їхніми реакціями, поведінкою в певних ситуаціях. Зокрема тематичний таргетинг, таргетинг за інтересами, а також геотаргетинг дає можливість працювати з окремими цільовими групами на безпечній відстані, здійснюючи цільову агітацію та пропаганду. За допомогою зазначених інструментів досвідчені фахівці спецслужб мають можливість дистанційно організовувати та координувати не тільки онлайн, але й офлайн події.

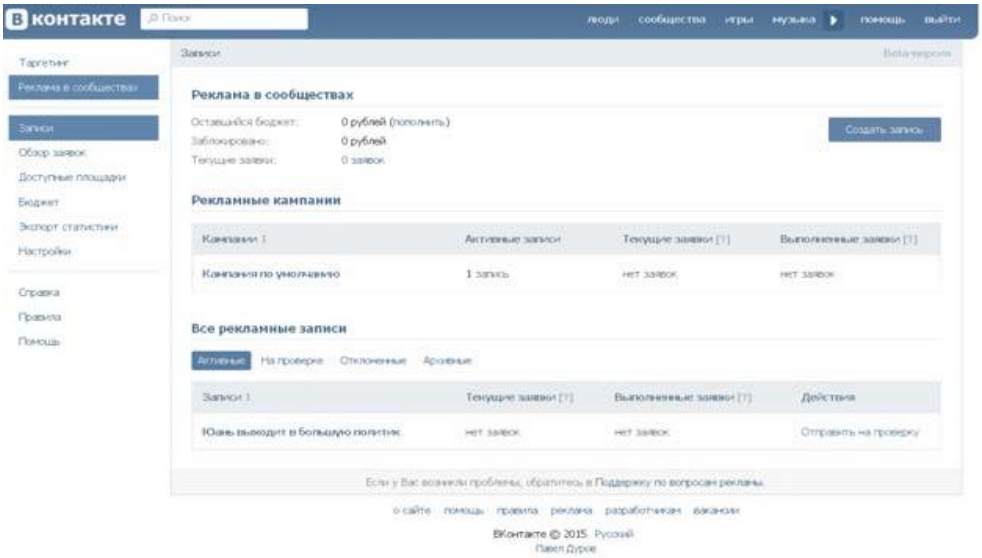
Практичний приклад

Класичним прикладом практичної реалізації таких можливостей стали події 13.10.14 р., коли на базі Нацгвардії в с. Нові Петрівці під Києвом 350 солдат-строковиків збунтувалися і пішки вирушили в столицю до Адміністрації Президента вимагати поліпшення умов служби та негайної демобілізації. В цьому випадку робота російських спецслужб здійснювалася через лідерів громадської думки в середовищі рядового складу підрозділу, шляхом налагодження контактів та здійснення впливу через соціальну онлайн мережу VKontakte.



Механізми використання таргетованої реклами прості та максимально автоматизовані. Рекламодавцю або замовнику не потрібно складати технічне завдання. Складання заявки здійснюється безпосередньо з персонального акаунту в режимі трьох кроків.

Перший крок – створення персонального кабінету, в якому формуються та зберігаються замовлення на рекламу (мал. 3.16.).



Мал. 30. Персональний кабінет рекламодавця

Кожна з соціальних онлайн мереж має певні особливості та специфіку процедури складання параметрів рекламної кампанії або дослідження, втім принципові положення подібні і відбуваються за єдиним, представленим вище, механізмом.

Окремий маркетинговий інструмент, що може бути задіяний в сучасній інформаційній війні,− це **контекстна реклама**.

Контекстну рекламу визначають, як принцип розміщення інформації, коли вона орієнтована на зміст інтернет-ресурсу, представлена у вигляді банеру чи текстового повідомлення.

Наприклад, на веб-сайті, присвяченому продуктам харчування, контекстна реклама пов'язуватиметься із поварами, споживачами або працівниками супермаркетів.

Однією із переваг контекстної реклами є геотаргетинг, що даєможливість обирати географію показу сторінок. Також застосовуються рамкові обмеження для часу показу. Ефективність контекстної реклами визначається рейтингом кліків (CTR) і вимірюється у відсотках [42, с. 22].

Специфічним видом контекстної реклами є пошукова реклама, яка розміщується в пошукових системах. Закладаючи ключове слово або словосполучення, користувач разом з необхідними матеріалами отримує посилання на рекламні оголошення або сайти, де певні товари або послуги рекламуються опосередковано. При цьому рекламне оголошення може з’явитися поруч із результатами пошуку (по боках або над даними).У випадку з текстовою рекламою, контекстна реклама розміщується блоками.

Головними провайдерами контекстної реклами є системи Google AdWords, Yahoo! Publisher Network та Microsoft adCenter.

Головною специфікою та особливістю контекстної реклами є принцип прив’язування інформаційного повідомлення до тематичних запитів користувача. В такому разі, при правильному складанні рекламного повідомлення, меседжі, закладені в посланні, легко досягатимуть свідомості користувачів. При цьому деструктивна або маніпулятивна складова вуалюється під виглядом реклами.

Необхідно зазначити, що використання інтернет-реклами в будь-якому її варіанті в якості інформаційної зброї в інформаційно-психологічних війнах, є досить специфічним, але доволі ефективним інструментом.

Головний принцип – здійснення інформаційної атаки там, де її користувач очікує менш за все (контекстна реклама) та вихід на персональний рівень стосунків (таргетована реклама).

У разі вдалого застосування таких інструментів навіть досвідчені фахівці не одразу можуть вирахувати наявність та спрямування атакуючих дій і своєчасно відреагувати. Крім того, така атака може сягати підсвідомого ментального рівня, що робить її ще більш небезпечною, ніж традиційні агітація та пропаганда.

Зважаючи на те, що серед провідних тем, навколо яких точаться інформаційні протистояння, є побутові питання, питання харчового забезпечення, послуг та товарів широкого вжитку, саме інтернет реклама може дати можливість належним чином замаскувати та максимально наблизити до актуальних потреб цільових груп, дії атакуючої сторони.

9. **Використання мобільних засобів зв'язку як інструмента інформаційної атаки**

Ще одним специфічним мережевим інструментом у сучасних комунікаціях можуть бути мобільні засоби зв'язку. В якості гаджетів використовуються класичні стільникові системи зв’язку, а також різноманітні месенджери та інші сервіси, що розмивають чітку лінію розмежування між Інтернетом та класичним стільниковим зв’язком.

У такому разі засоби комунікації можуть застосовуватися як в класичному варіанті (телефонна розмова), так із залученням до мережі Інтернет. Цей напрямок має назву – **мобільний маркетинг**− комплекс заходів, спрямованих на промоцію товарів або послуг із використанням засобів стільникового зв’язку.

Мобільній маркетинг є одним з самих дешевих та, разом з тим, найбільш таргетованих засобів комунікаційного просування. В його основі - ***послуги SMS-розсилки*** та деякі інтернет-технології (Viber, WhatsApp, Skype, Telegram, Line, Facebook Messenger, ICG та ін).

Останнім часом дедалі більшої популярності набувають **месенджери** - програми для швидкого обміну повідомленнями, розроблені для спілкування за допомогою мережі Інтернет. Відповідне програмне забезпечення встановлюється на персональних комп’ютерах або мобільних пристроях (смартфони, планшети). Сучасні месенджери дають можливість не тільки обмінюватися текстовими файлами, але й надають можливість голосового і відео зв’язку. При цьому, сучасні соціальні мережі можуть забезпечити достатньо високий рівень конфіденційності спілкування та передання даних.

Зазначений інструмент дає можливість донести комунікаційне повідомлення персонально, привернути увагу та налаштувати на певну дію конкретну особу.

Важливим аспектом класичної SMS-розсилки є її масовість – переважна частина користувачів є власниками мобільних телефонів.

Для розповсюдження інформації зазначеним засобом використовують бази телефонних номерів. Останні можна отримати різними шляхами: *офіційним* − адресат дає згоду на отримання рекламно-інформаційних SMS-повідомлень; *не офіційним* – розсилка спам-повідомлень. У цивілізованому світі існують певні законодавчі бар’єри, що блокують нав’язливу персональну рекламу, аж до кримінального переслідування.

Зазвичай адресні бази формуються в процесі здійснення купівлі (комерційна сфера) або при складанні баз даних по конкретним організаціям (державним, громадським, військовим структурам та ін.).

В умовах ведення військових конфліктів сучасні засоби радіоелектронної боротьби можуть забезпечити доступ до стільникового зв'язку, накриваючи окремі території.

Серед провідних технологій, що використовуються в мобільному маркетингу, визначають:

- голосові повідомлення;
- SMS-розсилки;
- MMS-розсилки (текстові або мультимедійні повідомлення, з можливістю використовувати фото, відео, музику, посилання та ін.);
- wap, gprs, edge та іншітехнології, що доступні для отримання інформації з мережі Інтернет за допомогою мобільного телефону;
- голосове меню (дозволяє тому, хто телефонує, спілкуючись із автоінформатором, отримати інформацію за потрібними темами, зробити замовлення, дізнатися про акції, знижки, промо-заходи та ін.);
- технології для створення додатків під відповідні мобільні платформи (Android, iPhone, WindowsMobile тощо);
- системи обміну миттєвими повідомленнями (спілкування, конференція, чат).

У форматі сучасної інформаційної війни використання всього спектру мобільних засобів комунікації – від стільникового зв'язку до різноманітних месенджерів набуває особливого значення. Зокрема використання звичайного розсилання SMS-повідомлень може застосовуватися як інструмент прямого або опосередкованого психологічного тиску на військовослужбовців.

Зокрема застосування такого інструмента ведення інформаційно-психологічної війни можна було спостерігати під час активізації бойових дій в Донбасі. За допомогою відповідних електронних пристроїв російська сторона робила розсилання повідомлень панічного характеру на мобільні пристрої українських військовослужбовців, що знаходилися безпосередньо в зоні бойових дій.

10. Соціальні онлайн мережі в системі сучасних форматів ведення війни

Трансформація технологій, специфіка соціальних, економічних та політичних умов розвитку сучасного світового співтовариства впливають на характер та особливості ведення сучасних війн.

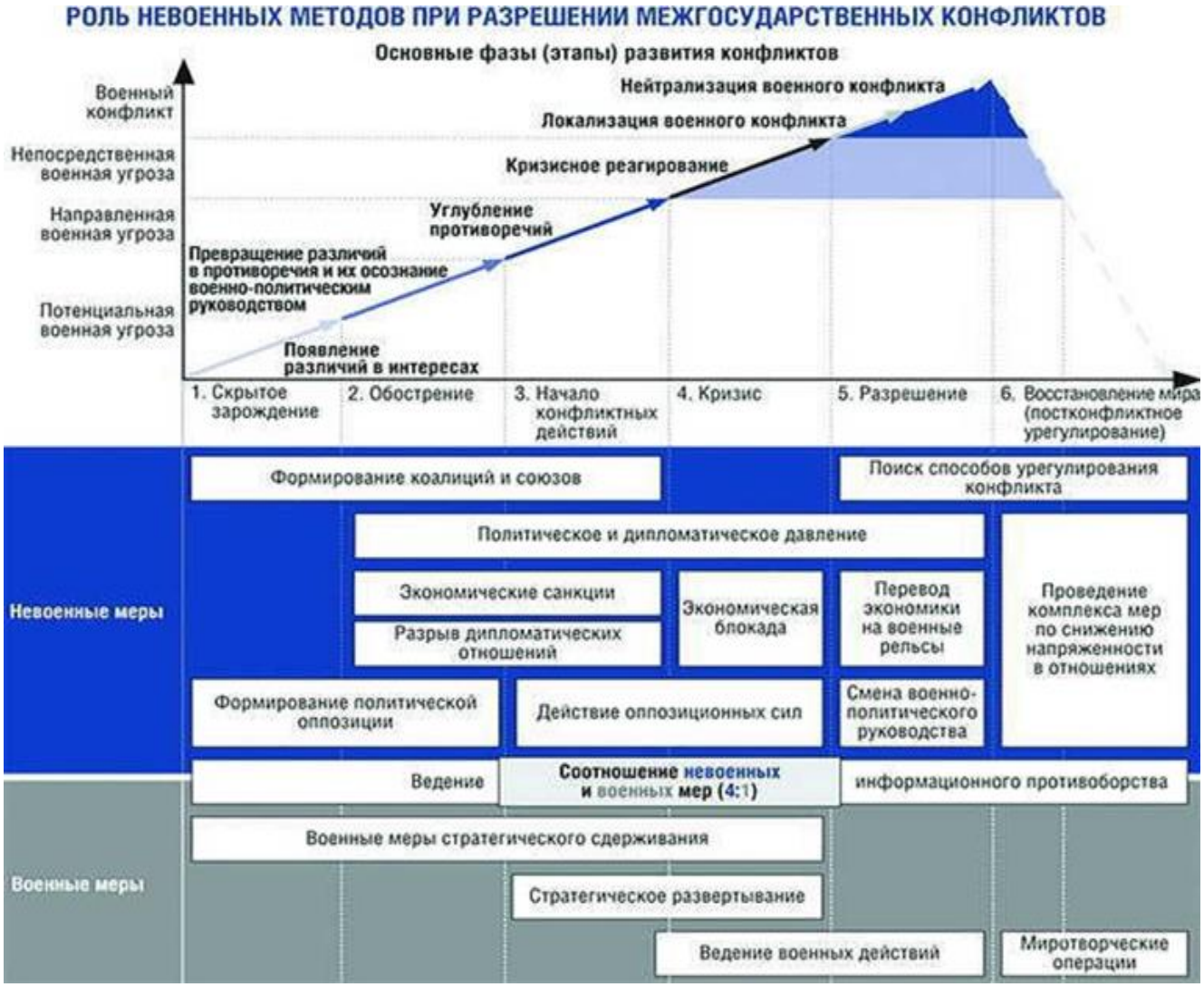
Провідні країни світу виділяють сьогодні на оборону значні бюджети, що дозволяють їм тримати мілліонні армії, мати найсучаснішу зброю, в тому числі таку, що відноситься до категорії зброї масового знищення. В цих умовах конфлікт двох або кількох таких країн, пов'язаних з іншими подібними країнами

різними угодами та союзами, може автоматично перетворитися на глобальну війну і, можливо, навіть до застосування ядерної зброї.

У таких умовах виникає потреба пошуку більш безпечного засобу вирішення конфліктних ситуацій, що не призведе до негативних глобальних наслідків. Таким засобом стала гібридна війна, яка являє собою комбіноване, інтегроване військово-політичне та економічне протистояння у вигляді безстатусного, часто прихованого, конфлікту.

Однією з провідних країн, яка активно використовує сьогодні інструменти гібридної війни, є країна-агресор − росія. Узагальнивши досвід гібридних конфліктів кінця XX – початку XXI ст., які вели США, провідні країни ЄС та азійського регіону, профільні російські фахівці розробили нову концепцію такого роду війн та застосували її на практиці проти своїх сусідів і намагаються боротися за відновлення системи двополярного світу, який існував за часів СРСР.

Базові складові частини російської стратегії і тактики сучасної гібридної війни були сформульовані в 2013 р. начальником генерального штабу ВС РФ В. Герасимовим (мал. 31.). Саме на основі цих принципів було сплановано та реалізовано напад на Україну, захоплення Криму та розв’язання війни в Донбасі. Серед ключових складових російської концепції зазначалися збільшення ролі невійськових методів тиску на противника, насамперед, за допомогою політичних (дипломатичних), економічних і гуманітарних елементів. Що стосується інформаційної складової, то вона визначалася як основа діяльності на всіх етапах конфлікту: його зародження, супроводу і в постконфліктний період. Особлива увага в Концепції відводиться і «асиметричним заходам», до яких були віднесені: діяльність підрозділів спеціального призначення; підтримка внутрішньої опозиції і колабораціоністів, а також збільшення цілеспрямованого інформаційного впливу на об'єкт нападу.



Мал. 31. Схема гібридної війни (російське бачення)

Послідовними, типовими складовими етапами гібридної війни в Концепції було визначено:

- **інноваційна агресія** (кібервійна, економічний тиск, інформаційно - психологічні атаки тощо);
- **застосування нерегулярних збройних формувань або приватних армій** (повстанський, партизанський рух, тероризм);
- **офіційні військові дії або демонстрація сили (**ідентифікована уніформа, зброя, офіційне визнання участі в конфлікті).

Аналізуючи перебіг багатьох гібридних конфліктів, дійсно іноді доволі складно виявити і тим більш ідентифікувати приховану економічну атаку, яка може бути замаскованою під виглядом конкуренції та боротьби за лідерство між країнами та транснаціональними корпораціями, в окремих секторах або галузях економіки. Так само не завжди в просуванні національної культури однієї країни на теренах іншої можна простежити акт агресії. Схожа ситуація має місце і в

просуванні ЗМІ, які здійснюють боротьбу за цільові аудиторії та зони впливу, що можуть поширюватися на сусідні держави та навіть окремі континенти.

Навіть уразі можливості відстеження зазначених тенденцій, вкрай важко обґрунтувати і довести звинувачення та змусити опонента припинити агресивні дії. До цього залучаються міжнародні третейські інституції, присуди яких виносяться роками та мають нечіткі рішення. Крім того, процедура прийняття рішень такими структурами є доволі тривалою, в той час, як гібридні атаки здійснюються швидко.

Етап інноваційної агресії іноді може бути розтягненим на роки і десятиліття. Класичним прикладом тому може бути така агресія росії проти України. Типовими ознаками її були газові і торговельні війни, намагання захопити стратегічні підприємства, поширити вплив власних ЗМІ, тиск на політичному рівні в питаннях захисту прав російськомовного населення, просуванні елементів російської культури (кіно, література, твори мистецтва тощо).

Саме на цьому етапі відбувається закладання конкретних масових психологічних установок, які згодом, у моменти переходу конфлікту до відкритої фази, використовують для послаблення сторони, проти якої здійснюється агресія.

В наступному етапі гібридної війни набуває характеру певної відкритості, з якого вже стає зрозумілим, хто є ініціатором агресії, втім з наведенням доказів у цьому випадку доволі складно, бо атакуюча сторона не розкриває остаточно своїх карт.

На цьому етапі головними **засобами здійснення гібридної агресії є**:

- створення атмосфери бездуховності, накручування конфліктних ситуацій, знищення авторитету державної влади;
- дестабілізація політичної ситуації (конфлікти, репресії, терор);
- блокування інформаційної діяльності органів центральної влади та місцевого самоврядування;
- підрив авторитету та дискредитація органів державної влади всіх рівнів;
- провокування соціальних, політичних, національних, релігійних зіткнень – аж до розв’язання громадянської війни;
- ініціювання масових акцій протесту та безладів на вулицях, погромів офіційних установ та громадських структур.

Фактично всі представлені вище засоби були випробувані російською стороною під час захоплення Криму, розпалювання війни в Донбасі та

дестабілізації ситуації в середині України з кінця 2013 р. і до початку широкомасштабного вторгнення.

Характерною ознакою цього етапу є застосування ***нерегулярних збройних формувань або приватних армій,*** які діють під виглядом партизанських груп, повстанських об'єднань або терористичних організацій.

У переважний більшості випадків тут держава-агресор може виказати себе через:

- офіційну політичну підтримку сепаратистських рухів на рівні публічних заяв чи через відстоювання інтересів повстанців у міжнародних установах;
- надання матеріально-технічної допомоги у вигляді техніки, зброї, продуктів харчування, коштів та інших ресурсів.

На цьому етапі держава-агресор у боротьбі із противником спирається вже не тільки на окремих інсайдерів та певні групи впливу в середині країни, проти якої здійснює агресію, але й починає застосовувати власні закамуфльовані війська або залучає приватні армії.

Так, у війні, яку розпалила росія на Сході України, були ідентифіковані такі угруповання, як:

1. *Козаки* (щось середнє між поліцією і солдатами).
2. *Військовослужбовці регулярної армії* («зелені чоловічки»).
3. *Чеченські найманці* (підрозділи створені А.Кадировим).
4. *Інші найманці* (представники арабських країни та деяких країн ЄС).
5. *Колишні співробітники "Беркута"* (розформований спецпідрозділ МВС України).
6. *Місцеві етнічні росіяни,* що живуть в Україні.
7. *Російські «туристи»* (колишні військовослужбовці, що діють як найманці).
8. *Реальні актори* (використовуються з ціллю пропаганди або навмисно шукають західні камери, щоб розіграти свою драматичну роль і висловити свою порцію пропаганди).
9. *Колишні українські солдати і офіцери* (дезертирували з української армії чи служать у ній і діють як зрадники / шпигуни).
10. *Місцевий криміналітет,* що пройшов навчання іотримав зброю.
11. *Місцеві жителі,* які були змушені воювати (через гроші, примус або під впливом пропаганди).
12. *Російські кримінальники або ув'язнені,* що потрапили під амністію в обмін стати найманцем в Україні.
13. *Агенти ФСБ.*

14. *Російські генерали та вищий офіцерський склад,* які «координують припинення вогню» на українській стороні фронту.

15. *Іноземні журналісти,* що збирають цінну інформацію та створюють негативні сюжети про Україну.

Що сьогодні собою являють *типові приватні армії,* можна зрозуміти, проаналізувавши діяльність потужних транснаціональних корпорацій, які для захисту своїх економічних інтересів залучають до співпраці певні незалежні озброєні групи або створюють власні формування.

Традиційно такі військові групи визначають, як ***приватні військові компанії*** (далі - ПВК) – комерційні підприємства, що пропонують послуги, пов'язані із охороною, захистом певних об'єктів або персон. Доволі часто вони беруть активну участь у військових конфліктах, а також здійснюють збирання розвідувальних даних, надають послуги із стратегічного планування, логістики та консультують.

У квітні 2001 р. була створена міжнародна організація «Peace Operations Association», головним завданням якої є координація та представництво інтересів усіх її членів на різних рівнях. Після початку війни в Іраку було створено «Private Security Company Association of Iraq» - асоціацію приватних військових та охоронних компаній, що контролювали ситуацію в цій країні. До складу зазначеної структури увійшло понад 40 компаній.

Серед прикладів типових послуг, які надають приватні армії, є такі, як:

- набір особового складу для контингенту міжнародних поліцейських місій та управління ними (DynCorp);
- охорона об'єктів, у тому числі тих, що мають важливе і стратегічне значення(так, "DynCorp" забезпечувала охорону стратегічно важливого нафтового резерву США);
- охорона нафтових родовищ і трубопроводів, охорона енергетичної системи (Hart Group, Black water Security Consulting, ErinysIraq Limited);
- охорона посольств та керівників держави (Triple Canopy);
- супроводження конвоїв ООН (Kroll);
- навчання особового складу урядових збройних сил, поліції та інших сил безпеки (так, у лютому 2002 року 70 співробітників ізраїльської компанії "Levdan" займалися навчанням збройних сил Конго);
- надання послуг військових перекладачів (CACI);
- охорона в'язниць (Titan Corporation);
- розмінування мінних полів та нищення боєприпасів (RONCO, MAG, BACTEC, Armor Group, Minetech, EODT);
- протипожежний захист (Group 4 Falck);

- тилове постачання військ (KBR);
- авіарозвідка (AirScans Inc., Eagle Aviation Services & Technology);
- збройний супровід і захист морських суден від піратів (Global Marine Security Systems).

Слід зазначити, що поступово роль і значення ПВК зростає. Приміром, станом на 2007 р. близько 25% усіх розвідувальних операцій для силових структур США забезпечували саме такі структури.

У західних країнах діяльність таких приватних військових структур чітко регламентується законом та контролюється. Сьогодні в світі сформувався чітко структурований ринок військових послуг із загальним обсягом у понад $100 млрд. Серед найбільш відомих сьогодні визначаються такі компанії, як: «Hulliburton», «Blackwater», «Dyn Corp», «Logicon», «Brown & Root», «MPRI», «ControlRisks», «Bechtel», «ArmorGroup», «Erinys», «Sandline International», «International Defenseand Security».

На відміну від європейської та американської практики в росії специфіка діяльності таких організацій має дещо інший характер. Перші приватні армії з'явилися в Росії в 2007 р., у складі компаній «Транснефть» та «Газпром» з метою захисту від зазіхань криміналу. Втім згодом вони перетворилися на неформальні силові структури, що діють під прикриттями та за настановами ФСБ і особисто кремлівського керівництва. Формально вони регулюються профільними нормативно-правовими актами, але в реальності їх діяльність повністю контролюється офіційною владою. Саме такі російські структури починали агресію в Донбасі та виконували допоміжні функції при захопленні Криму.

На заключному етапі гібридної війни боротьба фактично набуває відкритої форми і може перейти в офіційний збройний конфлікт.

Це здійснюється або у форматі відкритої інтервенції, або під виглядом введення миротворчих сил. В обох випадках головним офіційним приводом є намагання зупинити внутрішньо національні конфлікти або припинити неправомірні дії офіційної влади, що суперечать сучасним нормам та принципам захисту прав людини, встановленим та закріпленим у міжнародних угодах та деклараціях ООН, ЮНІСЕФ, Ради Європи тощо.

Маємо зазначити, що складні для офіційного контролю форми діяльності ПВК ідеально підходять для застосування у так званих ***гуманітарних інтервенціях***, що є типовою ознакою гібридної війни. Такі інтервенції визначають, як примусові дії особливої форми, які застосовуються міжнародною спільнотою або окремими державами.

Найбільш легітимним сьогодні, для здійснення миротворчих операцій або камуфлювання під них, вважається мандат Ради Безпеки ООН, який дозволяє:

- розгортання сил для запобігання конфлікту і його виходу через кордони;
- стабілізацію конфліктної ситуації після припинення вогню;
- створення умов для досягнення угоди про встановлення міцного миру між сторонами;
- забезпечення здійснення всеосяжних мирних угод;
- надання сприяння країн чи територій у подоланні перехідного періоду і створенні стабільного уряду на основі демократичних принципів, ефективного управління та економічного розвитку.

Слід зазначити, що саме наприкінці XX – на початку XXI ст. кількість таких гуманітарних інтервенцій зросла в рази, що можна пояснити такими факторами, як:

- зникнення біполярної конфронтації США та СРСР, яка ускладнювала діяльність Ради Безпеки ООН щодо питань санкціонування миротворчих операцій;
- різке зростання геополітичного впливу США та їх прагнення до встановлення власних правил гри на міжнародній арені;
- посилення тиску на слаборозвинуті країни, що володіють стратегічними ресурсами (газ, нафта та ін.) чи вигідним геополітичним положенням;
- наявність країн із антидемократичними режимами та терористичних організацій світового масштабу, з якими необхідно вести боротьбу;
- зміна норм міжнародного права щодо збільшення уваги до проблем захисту прав людини.

На відміну від загальновизнаного світовим співтовариством мандату на миротворчі операції, іноді країни агресори намагаються використовувати квазі мандати або локальні міждержавні угоди під прикриттям яких здійснюється окупація чужих територій. Саме так було, коли росія використала своїх «миротворців» у Придністров'ї (1992р.), Абхазії (1994р.), Південній Осетії (2008р.).

Специфіка та особливості сучасної гібридної війни стимулює створення нових форм військово-політичної агресії, які мають усі необхідні формальності або забезпечуються ґрунтовним юридичним прикриттям. Саме так відбулося під час захоплення Криму. Анексія частини української території була легітимізована через проведення «народного» «референдуму», волевиявлення під час якого контролювалося та забезпечувалося силами спеціальних операцій ЗС РФ.

При здійсненні російської агресії в Донбасі в 2014 році, кремлівське керівництво планувало застосувати технології миротворчої місії за мандатом

Організації договору про колективну безпеку (ОДКБ або Ташкентська угода). Втім реакція світової спільноти та економічні санкції завадили реалізації цих планів, і росія зупинилась на варіанті відкритої, але офіційно не визнаної військової агресії.

Після невдалих спроб здійснення фронтальних атак на позиції українських силовиків у Донбасі, як це було, приміром, під час п'ятиденної війни в Грузії, росія в Україні перейшла до іншої тактики – активності переважно в форматі діяльності диверсійно-розвідувальних груп та провокаційних артилерійських обстрілів. Також застосовується тактика партизанської боротьби.

Крім того, слід зазначити, що російські підрозділи в Донбасі сьогодні активно застосовують так звану тактику «трьох кварталів», що передбачає скомбінованість дій одного і того ж підрозділу, який в одному кварталі міста може виконувати загальновійськові функції, в другому – здійснювати поліцейські функції, в третьому – виконувати гуманітарні місії. Цю тактику ми сьогодні наочно спостерігаємо в діях «ополченських підрозділів» так званих «ДНР» та «ЛНР».

Інформаційна складова гібридної війни, на усіх її етапах несе в собі функції забезпечувального характеру. На першому етапі вона створює умови для виникнення конфліктної ситуації, на другому – забезпечує привід для опосередкованого втручання держави агресора у внутрішні справи атакованої країни, на третьому – створює відповідний медійний фон для легітимізації дій агресора.

У цьому разі цільовими групами для інформаційних атак є:

- цивільне населення, що знаходиться в зоні конфлікту;
- цивільне населення атакованої країни в цілому;
- цивільне населення країни-агресора;
- представники світової спільноти.

За змістом інформаційна складова гібридної війни має вигляд «війни сенсів» із застосуванням передових методів агітації та пропаганди. Зокрема активно використовуються так звані **симулякри**– ***образи, яких в природі не існує.*** Головна мета таких дій – нав'язати атакованій стороні бачення та психологічні установки, які допомагатимуть агресору в реалізації його планів.

У форматі зазначеного, особливої ваги набуває завдання встановлення контролю над інформаційним простором країни, проти якої здійснюється агресія, а також тих країн, які можуть якимось чином впливати на перебіг конфлікту.

В якості допоміжного засобу використовують діяльність різноманітних громадських структур – благодійних фондів, аналітичних центрів, культурних товариств та ін.

У контексті останнього особливого значення набувають технології web2.0, які надають атакуючій стороні – країні агресору, необмежені можливості у здійсненні впливу на населення країни, проти якої здійснюється агресія. При цьому згадані можливості мають широкий спектр – від впливу на масову аудиторію до здійснення інформаційного контакту на індивідуальному рівні, тобто адресний.

11. Сучасні інноваційні засоби ведення гібридних війн

В рамках сучасних гібридних війн, напрямок роботи із соціальними он-лайн мережами найближче всього стоїть до питань функціонування **структур інформаційно-психологічних операцій** (далі ІПсО) та так званих **сил спеціальних операцій** (далі ССО).

Польовий устав Армії США визначає інформаційно-психологічні операції, як планову пропагандистську та психологічну діяльність, розраховану на іноземні, ворожі, дружні або нейтральні аудитори, що здійснюється з метою впливу на їх відношення та поведінку у потрібному напрямку для досягнення політичних, та військових національних цілей.

Інформаційно-психологічні операції поділяються на стратегічні, оперативні та тактичні. Такі операції передбачають використання засобів масової інформації та допоміжну діяльність у мирний і воєнний час, котра має на меті послаблення престижу і впливу образу противника у ворожих, нейтральних або союзних країнах і зміцнення свого впливу та престижу.

Допоміжна діяльність передбачає:

- демонстрацію сили;
- підвищення ступеня бойової готовності військ;
- перекидання військ;
- програми громадянських дій;
- громадянську непокору;
- мітинги;
- демонстрації;
- програми в галузі освіти, сільського господарства і медицини;
- певні способи ведення бойових дій.

Кожен з названих видів діяльності може впливати на прийняття рішень політичних діячів або населення країн, обраних в якості об'єктів атакування. У війні з застосуванням звичайних засобів збройної боротьби інформаційно-

психологічні-психологічні операції можуть підвищувати бойову ефективність військ при збереженні незмінної їх чисельності. Такі операції, коли їх здійснення було розпочато завчасно і вони проводилися з високою ефективністю, можуть дозволити відмовитися від фактичного застосування військової сили.

Інформаційно-психологічні операції можуть проводитися у кризовій ситуації, доки справа не дійшла до військових дій, в інтересах консолідації громадської думки на підтримку цілей атакуючої сторони, щоб не вдаватися до введення регулярних військ на іноземну територію. Зазначені операції є також невід'ємною частиною заходів з тактичної дезінформації, забезпечення внутрішньої безпеки інших країн, підтримки миру, боротьби з тероризмом і інших спеціальних операцій.

- *Стратегічні інформаційно-психологічні операції* здійснюються в інтересах досягнення довгострокових цілей, покликаних створити сприятливу психологічну атмосферу для ведення військових дій. Такі операції зазвичай носять глобальний характер.
- *Оперативні інформаційно-психологічні операції* здійснюються в інтересах досягнення середньострокових цілей, на підтримку військових кампаній в рамках великих операцій. Об'єктом таких операцій зазвичай є населення певного регіону.
- *Тактичні інформаційно-психологічні операції* здійснюються в інтересах досягнення короткострокових цілей, на підтримку командирів тактичної ланки. Об'єктом таких операцій зазвичай є протистоїть угруповання військ противника.

Відповідно до специфіки та характеру завдань, на забезпечення яких орієнтуються зусилля сил ІПсО, вони супроводжують військові дії стратегічного, оперативного та тактичного рівнів.

Психологічні операції орієнтовані на підтримку військових дій стратегічного характеру використовуються для досягнення цілей національної політики або для демонстрації загрози застосування військової сили. Психологічні операції в підтримку стратегічних завдань ґрунтуються на використанні в своїх інтересах вразливих сторін іноземних урядів, збройних сил і населення для досягнення довгострокових цілей. Приміром в США, Національне військове керівництво країни, через Комітет начальників штабів видає директивні вказівки і зазвичай керує стратегічними психологічними операціями. Головнокомандувач на театрі війни (військових дій) сприяє їм шляхом спонукання політичного керівництва іноземних держав до підтримки позицій, які не суперечать національним цілям США і їх союзників.

Інформаційно-психологічні операції в підтримку військових дій оперативного рівня є проміжними між військовими діями стратегічного і тактичного рівнів. На цьому рівні здійснюються планування і ведення військових кампаній і великих операцій у відповідному театрі військових дій. В практиці армії США, командувачі збройними силами та їх штаби зазвичай планують і проводять військові кампанії. Групи армій і армії, як правило, розробляють великі операції сухопутних військ, які ведуться армійськими корпусами і дивізіями. Хоча поняття «командир оперативної ланки» зазвичай асоціюється з головнокомандувачем збройними силами на театрі, немає такої ланки командування, яке прив'язувалася б до оперативного мистецтва. Відповідальність за дії військ на оперативному рівні може змінюватися в залежності від характеру військових завдань, розмірів і географічних особливостей театру війни, а також чисельності і концентрації військ.

На оперативному рівні сили психологічних операцій надають підтримку виходу в райони зосередження формувань звичайних збройних сил і їх тилового забезпечення; наземним і повітряним маневреним силам; ведення вогню з використання засобів ураження, а також діям сил спеціальних операцій. Основні особливості пропаганди та психологічних акцій, здійснюваних в рамках психологічних операцій, полягають в тому, що вони прямо або опосередковано сприяють поразці сил противника, викликаючи в нього невіра в можливість перемогти і примушуючи до відступу.

Психологічні операції в підтримку військових дій тактичного рівня відносяться до загальних завдань командира польового підрозділу, що передбачають знищення сил противника або пряме припинення його намірів. На цьому рівні армійські корпуси, дивізії або частини і підрозділи використовують специфічні способи або методи дій. Психологічні операції в підтримку військових дій тактичного рівня плануються і здійснюються в інтересах досягнення найближчих або короткострокових цілей. Психологічні операції можуть сприяти досягненню наступних тактичних цілей:

- ізоляції живої сили, техніки і матеріальних засобів супротивника;
- безпосередньої вогневої підтримки;
- розвідці і спостереження;
- вибору позицій і передислокації систем зброї.

Психологічні операції в підтримку військових дій тактичного рівня включають використання візуальної, звукової та відео-звукової техніки для надання безпосередньої підтримки в бойових частинах і підрозділах. Психологічні операції на цьому рівні плануються з розрахунком здійснення

впливу на цивільний і військовий персонал противника в зоні відповідальності командира тактичної ланки.

Конкретно взята категорія психологічних операцій (стратегічна, оперативна, тактична) може проводитися на підтримку більш ніж одного будь-якого рівня військових дій. Спільні завдання і цілі можуть служити для розмивання чітких меж між різними категоріями психологічних операцій.

Головна умова успіху в реалізації ІПсО − на будь-якому рівні психологічні операції повинні проводитися за єдиним задумом, з метою полегшення проведення військових операцій, зниження перешкод з боку цивільного населення і завоювання його підтримки. Ці операції повинні бути винахідливими, інтерактивними, проводитися в інтересах зниження ефективності і підриву лояльності військ противника, дії якого заважають досягненню поставлених цілей.

У структурі військових сил армії США, підрозділи ІПсО мають в своєму складі команди 27 різних типів. Така організація дозволяє командиру, що координує психологічні операції, створювати спеціалізовані частини і підрозділи для вирішення конкретних завдань.

Всі команди умовно можна розділити на три категорії − *управління, оперативні, постачання та обслуговування.* Ці команди, в свою чергу, об'єднуються в частини і підрозділи ІПсО трьох типів − *група, батальйон і рота.* Склад частин і підрозділів може бути різним у залежності від поставленого завдання.

З метою забезпечення максимальної гнучкості у виконанні поставлених завдань, частини і підрозділи ІПсО ВС США можуть надаватися загальновійськовим формуванням або здійснювати їх загальну або безпосередню підтримку в залежності від вимог. Вони можуть також передаватися в оперативне підпорядкування загальновійськових формувань. В усіх випадках частини і підрозділи ІПсО отримують директивні вказівки щодо ведення інформаційно-психологічних операцій і спеціальне тилове забезпечення по зовнішніх каналах психологічних операцій.

Групи ІПсО загальної підтримки зазвичай надаються або виділяються для супроводження підрозділів сухопутних військ в зоні бойових дій. При цьому батальйон ІПсО загальної підтримки, в зоні військових дій використовують з метою досягнення стратегічних та оперативних цілей, а також для здійснення пропаганди серед цивільного населення.

Спеціально навчені і підготовлені батальйони психологічних операцій можуть бути передані в оперативне підпорядкування командування військової

поліції по роботі з військовополоненими для забезпечення порядку в таборах військовополонених.

В переважній більшості випадків, директивні вказівки щодо ведення психологічних операцій надходять з штабу групи психологічних операцій. Батальйони ІПсО, безпосередньої підтримки надаються для підтримки армійських корпусів; роти безпосередньої підтримки – для дивізії або окремої бригади. Накази з проведення психологічних операцій вони отримують від штабу групи ІПсО, яка надається або підтримує угруповання військ в зоні військових дій.

Частини та підрозділи ІПсО розробляють кампанії з метою підтримки звичайних збройних сил і сил спеціальних операцій, використовуючи такі інструменти, як:

- аналіз завдання підтримуваного об'єднання (з'єднання, частини);
- визначення завдання психологічної операції;
- збір інформації та моніторинг ситуації;
- аналіз об'єкта на який здійснюється вплив;
- вибір тем і символів;
- вибір засобів поширення інформації;
- підготовка інформаційних матеріалів;
- попередня перевірка ефективності запланованих заходів;
- отримання остаточного дозволу на проведення кампанії;
- реалізація операції;
- оцінка ефективності пропагандистських заходів.

В армії США відповідальність за узгодження психологічних операцій в процесі вироблення рішення покладається на начальника оперативного управління (відділу, відділення) відповідного штабу. Саме він зобов'язаний планувати проведення психологічних операцій при підготовці будь-якої військової операції і починати їх планування завчасно, одночасно з оперативним плануванням. Завчасне планування дає можливість синхронізувати зусилля особового складу частин (підрозділів) ІПсО з проведенням військової операції, щоб створити найбільш сприятливі умови для досягнення успіху.

У контексті гібридних технологій ведення сучасних військових протистоянь особливе значення мають так звані **сили спеціальних операцій** (далі ССО) та специфіка їх комунікаційного, в тому числі за допомогою соціальних онлайн мереж, забезпечення.

У країнах євроатлантичного блоку головним призначенням сил спеціальних операцій є протидія асиметричній агресії, боротьба з тероризмом, партизанським рухом та здійснення психологічного і територіально-

адміністративного впливу на населення певних територій, на яких розгортаються важливі події.

За визначенням, сили спеціальних операцій – ***підрозділи спеціально навчених фахівців,*** які мають спеціальні можливості в сферах розвідки, прямих акцій і військової підтримки для виконання складних, небезпечних, інколи політично чутливих операцій, що проводить командування.

Під **спеціальними операціями** розуміють різновид військової діяльності, яку здійснюють спеціально створені сили, організовані, треновані та оснащені для цієї мети, що використовують оперативну техніку й методи, відмінні від традиційних військових.

Підсумовуючи викладене добавимо, що характерними ознаками ССО є:

- прихованість дій;
- здатність виконувати операції, котрі приводять до тактичної або стратегічної переваги;
- спеціальна навченість та оснащеність;
- високий рівень спеціалізації;
- підвищений рівень адаптованості;
- мобільність й здатність проводити операції автономно;
- відносно невелика кількість особового складу;
- спроможність працювати в трьох середовища (повітря, земля, море).
- До типових завдань ССО відносяться:
- рейди та сучасні бойові дії;
- психологічні операції (Psy-Ops);
- робота «цивільної адміністрації» (залучення на свій бік населення);
- навчання іноземних армій, поліційних і без пекових сил (так зване «примноження сили»);
- пошук, евакуація й доставка полонених, заручників;
- медична допомога;
- здобуття розвідувальної інформації за лінією фронту;
- виявлення, ідентифікація та визначення цілей для власних засобів ураження;
- антитерористичні операції.

У своєму розпорядженні євроатлантичні ССО мають розгалужену інфраструктурну мережу «глобальної присутності» та «передового базування» - сухопутні оперативні бази, координаційні центри та морські склади-платформи.

Безумовним лідером у питаннях створення та застосування ССО серед країн євроатлантичного блоку є США. Для координації власних підрозділів та

ССО союзників при військовому відомстві США створено Командування спеціальних операцій (USSOCOM), основними завданнями якого є :

- координація діяльності ССО США;
- планування та проведення спеціальних операцій;
- організація бойової підготовки та підтримки в належному стані підрозділів ССО.

Крім провідних терористичних організацій, головним опонентом США та його союзників у питаннях застосування ССО сьогодніє російська федерація.

Створені в 2009 році російські ССО – це високо мобільне, спеціально технічно оснащене, добре екіпіроване армійське угрупування сил міністерства оборони рф, призначене для спеціальних завдань (при необхідності застосування військової сили) як в середині країни, так і за кордоном з метою захисту інтересів країни-агресора, що знаходяться в постійній і високій готовності до застосування.

За структурою, функціями та практичним призначенням російські ССО мало чим відрізняються від євроатлантичних, хіба що вони не на стільки якісно забезпечені озброєнням та засобами комунікації.

Широкому колу російські ССО знайомі під назвою «зелені чоловічки» з часів початку агресії проти України –захоплення Криму та міст на сході країни.

Саме ці підрозділи стали основою для формування незаконних збройних формувань так званих формувань «ДНР» і «ЛНР» у вигляді «ополчення» та різноманітних сепаратиських «бригад» та «батальйонів».

В Україні в 2015 році було розпочато процес створення власних ССО за стандартами НАТО. Каталізатором цього рішення стала російська агресія та війна сході країни.

Серед завдань українських ССО є:

- спеціальна розвідка;
- спеціальні заходи;
- контр терористичні заходи;
- прямі військові дії;
- аналіз і обробка інформації для вироблення правильної стратегії та залучення необхідних ресурсів;
- нетрадиційні методи ведення війни –психологічні та інформаційні операції.

Згідно з концепцією і законопроєктом, підготовленими експертами Центру оборонної реформи, організаційно ССО будуть складатися з різних департаментів: інформаційно-психологічних операцій, інформаційно-аналітичної роботи, технічної підтримки і декількох бойових підрозділів. У

складі ССО буде і управління нетрадиційних методів ведення війни, яке відповідатиме за створення руху опору, партизанських загонів, підпільних організацій. Також буде створено логістичний підрозділ і окремий навчальний центр.

Новостворене Командування ССО, за штатним розкладом, очолює керівник із військовим званням генерал-лейтенант. Перший заступник командувача — командувач високо мобільних десантних військ (у званні до генерал-майора), як можна побачити з назви посади керує частинами ВДВ у складі ССО ЗС України.

Відповідно до наявної інформації можна приблизно передбачити структуру Сил спеціальних операцій:

- командування ССО,
- командування ВДВ (у складі КССО),
- 140-й центр спеціального призначення,
- 73-й морський центр спеціального призначення,
- 3-й окремий полк спеціального призначення,
- 8-й окремий полк спеціального призначення,
- 25-а повітряно-десантна бригада,
- 79-а окрема аеромобільна бригада,
- 80-а окрема аеромобільна бригада,
- 81-а окрема аеромобільна бригада,
- 95-а окрема аеромобільна бригада.

Отже, весь наявний потенціал і комунікаційні можливості соціальних он-лайн мереж можуть стати важливим інструментом у діяльності ССО. Відповідно в структурі окремих підрозділів та керівних органів ССО мають бути фахівці і навіть групи, які забезпечуватимуть відповідні функції.

Особливої ваги це набуває в контексті наукового прогресу та вдосконалення технічних засобів комунікації, які дозволятимуть мати доступ до мережі Інтернет за умови значного віддалення від стаціонарних місць доступу та зберігання такої можливості протягом тривалого часу.

12. Інтернет-технології та соціальні онлайн мережі в структурі гібридної війни

Як вже зазначалося вище, головним завданням мережевих онлайн проектів у рамках гібридної війни є створення певної віртуальної реальності (симулякри), що формує необхідне для атакуючої сторони бачення ситуації конкретними цільовими групами, які є об’єктами інформаційно-психологічної агресії. При цьому, головною метою такої діяльності є забезпечення сприятливих умов для

реалізації атакуючих дій в режимі оф-лайн, на економічному, військовому, політичному полях, або одночасно в усіх площинах.

Вирішення зазначених питань можливе лише за умови інтегрованого підходу – поєднання сучасних технічних комунікацій та психотехнологій. При цьому, тривалість дії та глибина ударного ефекту залежать від часу, впродовж якого здійснюється обробка свідомості цільових груп та потужності тиску. Роль і значення в цих процесах соціальних онлайн мереж важко переоцінити.

За аналогією, технології web 2.0, в цьому контексті можна визначити як високоточну зброю, що може поцілити не просто в певні цільові групи, але й в конкретних її представників, чітко визначених персоналій. Така адресність та, за необхідністю, вибірковість дає можливість досягати максимального ефекту із оптимізацією витрат у плані часу, інтелектуальних та матеріально-технічних ресурсів.

Аналізуючи результати найбільш відомих міжнародних військових, політичних та економічних конфліктів кінця XX – початку XXI ст., стає зрозумілим, що інформаційно-психологічна зброя сьогодні має бути прирівняна до зброї масового знищення. Не вбиваючи фізично, психотехнології стають причиною групових, а також масових психічних розладів, що призводять до соціальних конфліктів, в яких позбавляються життя конкретні індивідууми.

У форматі використання всього спектра інформаційно-психологічних операцій соціальні онлайн мережі мають можливість забезпечувати:

- координацію протесту та терористичних рухів;
- поширення контенту, що відноситься до категорії інформаційної зброї;
- збирання важливої інформації про персон або організації,
- що представляють інтерес для атакуючої сторони;
- збирання розвідувальної інформації про офлайн дії противника;
- відстеження суспільних настроїв;
- локалізація джерел інформації, що представляють небезпеку.

Однією з головних функцій соціальних онлайн мереж є можливість координації інформаційних потоків, що розгортаються навколо реальних військових дій.

У сучасних умовах як гібридних, так і лінійних військових конфліктів важливе значення має система доступу до інформації, що надходить із зони бойових дій. А головним завданням будь-якої профільної військової структури є обмеження доступу до джерел інформації сторонніх осіб і поширення інформації у вигідному для себе контексті.

У контексті реалізації зазначеного вище завдання, роботу із соціальними мережами необхідно вибудовувати, базуючись на принципах встановлення

контролю трьох інформаційних потоків, які мають місце навколо будь-якого об’єкта, в якості якого в даному випадку виступатиме зона бойових дій.

Для чіткого розуміння процедури здійснення контролю за рухом інформації, необхідно скласти карту інформаційного поля, на якій змоделювати спрямування та складові частини трьох базових інформаційних потоків: ***вхідного***, ***вихідного*** та ***внутрішнього***.

Кожен з визначених інформаційних потоків формують певні джерела інформації або інформаційні носії, які мають певний контент та механізм його накопичення, зберігання та поширення і в цілому формують загальні обриси та структуру профільного інформаційного процесу. Серед тих, що відносяться до онлайн мережевих соціальних структур можна виділити такі, як:

- мережеві групи та сторінки центральних органів державної влади;
- мережеві групи та сторінки органів місцевої влади;
- мережеві групи та сторінки координаційних центрів громадських структур (волонтери, ГО, БФ та ін.);
- мережеві групи та сторінки окремих силових підрозділів;
- мережеві групи та сторінки координаційних центрів силових структур (штаби, логістичні центри, центри надання допомоги);
- мережеві групи та сторінки місцевих ЗМІ;
- мережеві групи та сторінки територіальних громад.

Для цих інформаційних потоків визначаються певні цільові групи. Зокрема для вхідного та внутрішнього **інформаційних потоків такими цільовими групами** будуть:

- цивільне населення в зоні конфлікту;
- керівництво місцевих органів влади;
- силовики (військові та поліцейські структури);
- волонтерські структури (благодійні або громадські організації);
- представники ЗМІ (власні та іноземні);
- офіційні спостерігачі (військові та цивільні місії).

Для контенту, що рухається за вихідним інформаційним потоком, **цільовими групами** будуть:

- цивільне населення, що мешкає поза зоною конфлікту;
- керівництво центральних органів влади;
- національні та іноземні медіа;
- представники національних та міжнародних громадських організацій;
- керівництво та представники іноземних державних установ.

Карта інформаційного поля в кожній конкретній ситуації формується індивідуально, на основі визначених вище елементів, із врахуванням місцевих особливостей та специфіки.

Для перетворення такої моделі в реально діючий механізм також необхідно визначити принципи та правила контролю і фільтрації інформаційних потоків. Під час роботи із соціальними мережами це завдання є доволі складним, бо потенційним джерелом інформації може виступити фактично кожна людина, яка має доступ до мережі Інтернет і володіє певним цінним контентом.

У такому разі необхідно налагодити систему регулярного моніторингу всього локального мережевого інформаційного простору в ручному (перегляданння змісту профільних сторінок та груп) або за допомогою відповідних програмних сервісів.

Крайньою мірою контролю за мережевою складовою зони конфлікту може бути блокування доступу до певних інтернет-ресурсів та мереж, утім, як свідчить практика, в наші часи це майже не реально. Тому, найкращий засіб контролю за інформаційним процесом–координування інформаційних потоків та формування правильних меседжів із відповідним контентним супроводженням.

Також ефективним засобом посилення власних можливостей щодо координації інформаційних потоків може стати залучення до активної співпраці волонтерів.

Волонтерський рух в онлайн мережевому середовищі, в якості інструмента протидії інформаційної агресії або для здійснення аналогічних атак на інформаційне поле супротивника, став одним із засобів протидії російської агресії проти України. В принципі світова практика інформаційних війн знає багато таких прикладів.

Практичний приклад

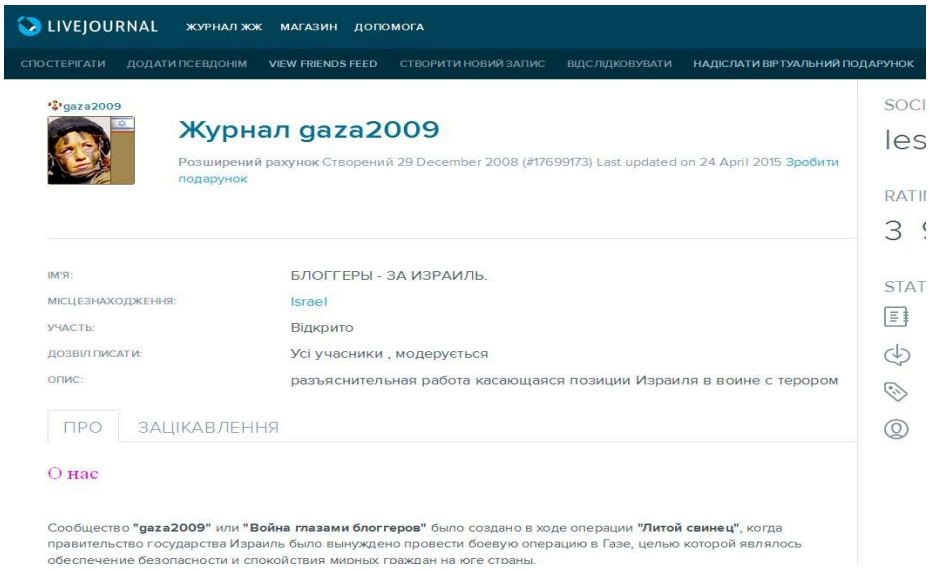
За прикладом використання соціальних мережевих онлайнструктур для забезпечення військового протистояння із залученням волонтерського компонентну, можна звернутися до досвіду інформаційного супроводження військової операції «Литий свинець», що здійснювалася Ізраїлем в секторі Газа в 2009 р.

Ця віртуальна інформаційно-психологічна операція стала однією з найперших та найуспішніших у своєму роді.

Унаслідок програного інформаційного протистояння під час Другої Ліванської війни (2006 р.) ізраїльське керівництво вирішило посилити інформаційний сегмент в структурі ЦАХАЛ та його щільну співпрацю із громадськістю. До співпраці, окрім офіційних ЗМІ, було залучено волонтерів,

головним завданням яких було відстежувати інформацію, що з'являлася у соціальних мережах, та поширювати контент, який дає об'єктивну інформацію про перебіг подій і показує діяльність ізраїльських військових у вигідному для них контексті. Також волонтерські групи та окремі блогери орієнтувалися на виявлення та нейтралізацію джерел (інтернет-майданчиків) противника.

Реальні бойові дії розпочалися 27 грудня 2008 р. і вже з перших днів січня 2009 р. провідні блогери-волонтери відкрили у найбільш популярній на той час соціальній мережі LiveJornal.com групу «gaza2009». Модераторами цієї групи Стали Марк Бибичков (радник міністра обороніІзраїля) та Давід Ейдельман (прес-секретар політичної партії «Кадима»).



Зазначена група стала майданчиком, навколо якого відбулася консолідація громадськості, а також джерелом інформації для світових медіа. Модераторам вдалося досягнути рівня відвідуваності до 30тис. на день,щ она ті часи та для цієї соціальної мережі було безумовним рекордом.

Крім того, зазначена група виконувала функції віртуального штабу. У разі виявлення джерел ворожої пропаганди модератори збирали усіх волонтерів та давали адресу місця, де відбувається ворожа інформаційна атака. Також фоловери групи виявляли та розвінчували фейки, поширюючи викривальну інформацію. Через певний час аналогічні групи було створено у мережах Facebook, Odnoklassniki, VKontakte.

Станом на січень 2010 р. ця діяльність перетворилась на глобальний рух, який допоміг ізраїльським військовим в плані комплексного інформаційного супроводу.

Серед аналогічних українських волонтерських проектів, які діють в якості допоміжних віртуальних ресурсів у інформаційно-психологічній війні з російськими агресорами та сепаратистськими рухами можна визначити такі як:

«Inform Napalm» та «Информационное сопротивление», центр «Миротворець». Практично всі згадані вище проекти діють за схемою роботи так званої **OSINT (Open source intelligence)**– ***розвідувальної практики, яка передбачає пошук, вибір та збирання інформації, отримано її з відкритих джерел.*** Важливою складовою частиною такої роботи є системний аналіз наявної інформації із відповідною оцінкою та висновками, що дозволяють зрозуміти логіку та передбачити дії противника.

Одним з базових золотих правил такої практики є те, що близько 90% необхідної для аналізу та прийняття відповідних рішень інформації знаходиться у відкритих джерелах. До таких джерел можна віднести:

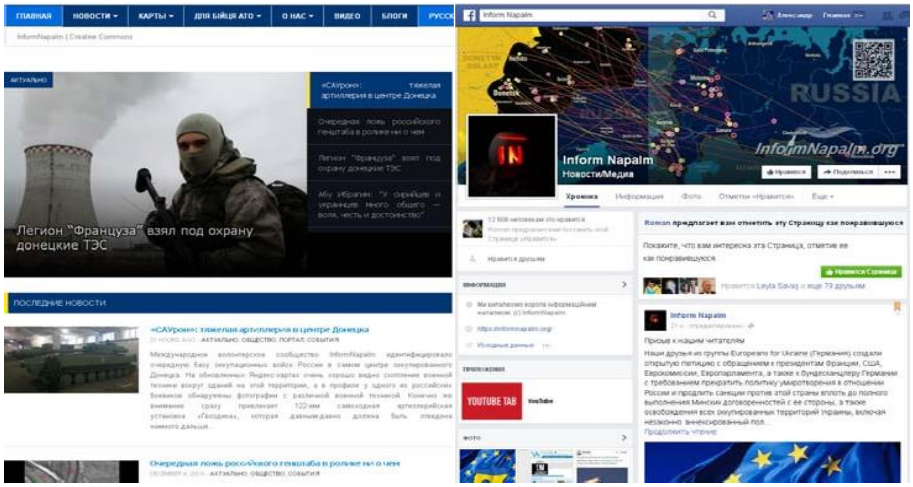
- традиційні ЗМІ (газети, журнали, радіо, телебачення);
- інтернет-видання, що відносяться до ЗМІ (сайти новин та портали, інтернет-ресурси профільних структур);
- аканти та віртуальні майданчики в соціальних онлайн мережах;
- офіційні звіти державних структур;
- публічні заяви політиків та державних службовців;
- спостереження — радіомоніторинг, використання загальнодоступних даних, аерофотозйомок (наприклад, Google Earth);
- професійні та академічні звіти, конференції, доповіді, статті;
- звіти та виступив ЗМІ окремих незалежних експертів та експертних груп.

У провідних країнах світу система OSINT є важливим інструментом захисту національних інтересів та провідною складовою в діяльності профільних силових відомств. Зокрема в США та країнах НАТО існуютьокремі мережі центрів, що займаються збиранням та обробкою відповідної інформації із подальшим формуванням відповідних баз даних та практичним їх застосуванням для прийняття відповідних рішень.

«Inform Napalm» *– громадський проєкт з інформаційного висвітлення подій, що стосуються неоголошеної війни Росії проти України, окупації Криму і терористичної діяльності російських спецслужб, а також фанатично налаштованих бойовиків "ДНР", "ЛНР", "Новоросії". На волонтерських засадах в команду "Inform Napalm" увійшли колишні військові, журналісти, аналітики, перекладачі та активісти. У мирному житті кожен з нас представляє самі різні професії, але з приходом війни в Україну вони всі стали солдатами інформаційного фронту.*

На теперішній час серед волонтерів проекту є ті, хто знаходиться в зоні АТО в якості військовослужбовців. Також до співпраці залучаються місцеві мешканці територій, які знаходяться під окупацією.

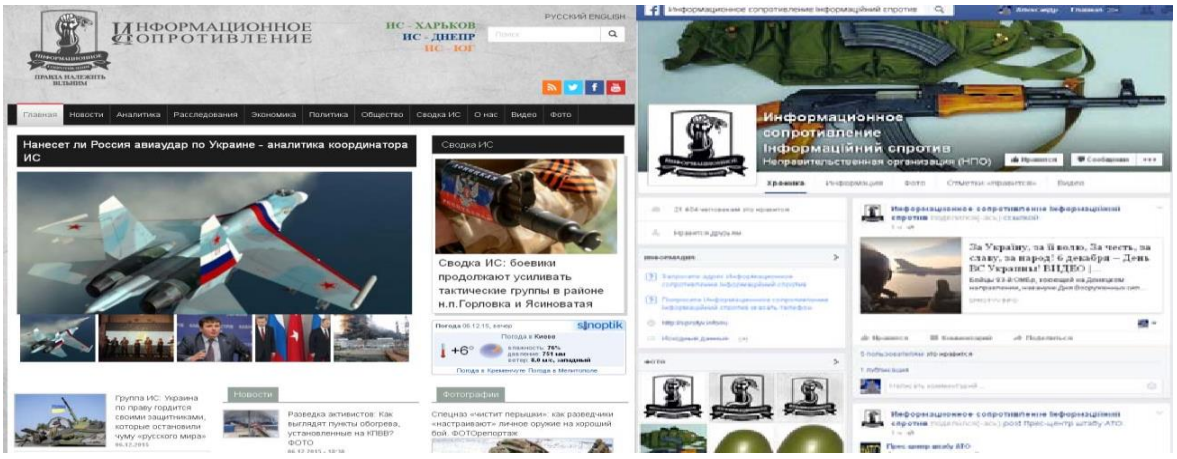
Серед матеріалів, які активісти проекту публікують, є фото та відео матеріали, офіційні документи, свідчення очевидців, що підтверджують російську агресію та розкривають військові злочини бойовиків ДНР-ЛНР.



«Информационное сопротивление» - *неурядовий проєкт, головним завданням якого є протидія в інформаційному полі зовнішнім загрозам, що виникають для України в основних сферах: військовій, економічній та енергетичній, а також у сфері інформаційної безпеки.*

Проєкт функціонує як ініціатива неурядової організації «Центр військово-політичних досліджень» (м. Київ). Початок роботи проєкту з 2 березня 2014 (з вторгнення росії до Криму).

Матеріали, що публікують на сайті та мережевих сторінках проєкту, це візуальні (фото та відео) матеріали, офіційні документи, свідчення та коментарі очевидців, які надають докази російської агресії та злочинів керівництва ДНР-ЛНР.



Також одним з найважливіших та найпопулярніших ресурсів є портал.

***«Миротворець»**, створений групою вчених і фахівців з питань дослідження ознак злочинів проти національної безпеки України, миру, безпеки людства та міжнародного правопорядку, що займаються творчою науковою та журналістською діяльністю.*

Волонтерами центру здійснюється фіксація і зберігання інформації щодо об'єктів дослідження, в діях яких присутні ознаки злочинів проти національної безпеки України, життя і здоров'я людини, миру, безпеки людства та міжнародного правопорядку.

Основними джерелами інформації, використовуваними Центром «Миротворець» для проведених наукових досліджень, є відкриті для загального доступу матеріали, які друкуються і розміщуються: в соціальних мережах, в web-виданнях, на приватних web-сторінках, в спеціалізованих форумах і блогах, транслюються по каналах телебачення і радіомовлення.

Зазначені вище вітчизняні мережеві проекти, демонструють яскравий приклад того, як за допомогою належним чином розбудованої інформаційної мережі та системи роботи можна ефективно забезпечувати та результативно супроводжувати офлайн процеси.

Таким чином, стає зрозумілим весь спектр наявних на теперішній момент інструментів ведення інформаційної війни, головний принцип яких гнучкість, оперативність та масштабність процесів, системність роботи. І лише від тих, хто приймає відповідні управлінські рішення, залежить наскільки якісно ці інструменти можуть спрацьовувати.

13. Мережеві онлайн проєкти в гібридній війні: структура та принципи функціонування

Одним з базових напрямків роботи в рамках інформаційної війни в соціальних онлайн мережах є **тематичні проєкти**. Останні мають монотематичне спрямування, гнучку схему управління та принципи і схеми розбудови комунікацій із відповідними, чітко визначеними цільовими групами.

За теоретичним визначенням «проєкт» – ***це сукупність дій та завдань, що внаслідок їх унікальності й неповторності*** має такі відмінні ознаки, як[184, с. 8]:

- чіткі цілі, що досягаються одночасним виконанням певних технічних, технологічних та інших вимог;
- внутрішні та зовнішні взаємозв'язки завдань, робіт, операцій і ресурсів, що потребують чіткої координації в процесі реалізації проекту;
- визначені терміни початку й завершення проєкту та обмеженість ресурсів;
- визначений ступінь унікальності проекту та умов його здійснення.

За складністю визначаються [184,с.10]:

- монопроєкти – окремі конкретні проекти чітко визначеної орієнтації та масштабу; припускають певні спрощення щодо проектування та реалізації, формування команди проекту тощо;
- мультипроєкти – комплексні проекти, які складаються з монопроектів;
- мегапроекти – комплексні проекти, які охоплюють окремі регіони, сектори суспільства, економіки; складаються з моно- і мультипроєктів, об'єднаних однією метою.

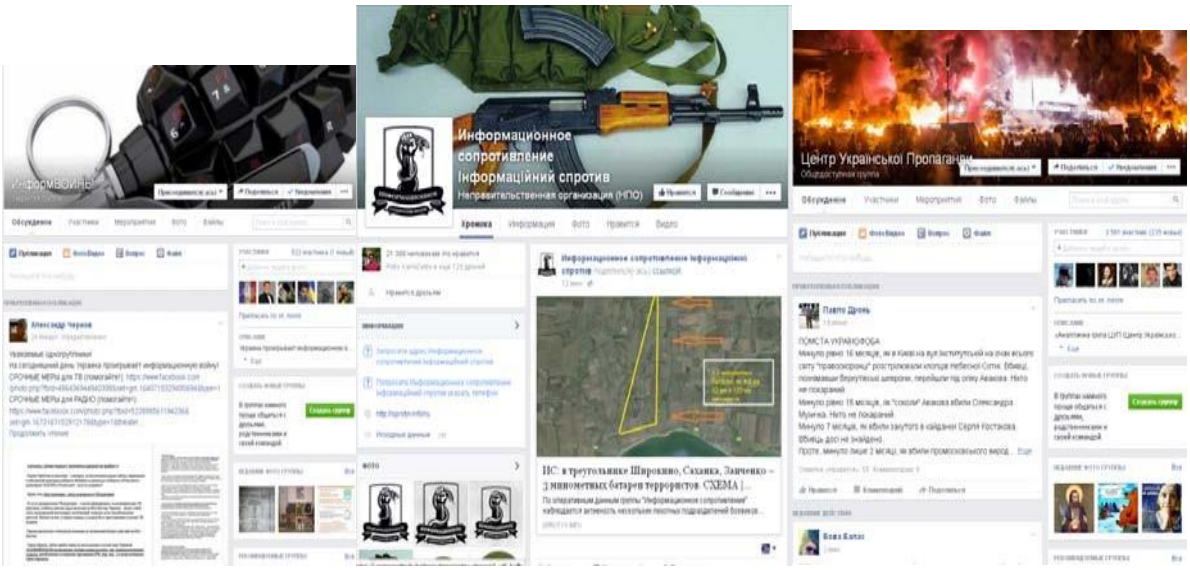
У контексті функціонування мережевого онлайн простору, в якості засобу ведення інформаційної війни, може використовуватися будь-який формат і тематика проектів. Головна вимога до таких проєктів – наявність прямого доступу до конкретних цільових груп, а також можливість здійснення прямого або опосередкованого впливу та безперешкодного функціонування.

Формат мережевих проєктів може бути у вигляді блогів (авторські або тематичні),груп(авторські,тематичні,регіональні,корпоративні),сторінок (авторські, тематичні, регіональні, корпоративні), подій (разові івенти). При цьому їх спрямованість може мати прямий (відкритий) або опосередкований (прихований) характер.

Мережеві онлайнпроєкти відкритого формату орієнтовані на цільові групи, що підходять під категорії своїх та нейтральних. З такими цільовими групами можна працювати, не приховуючи власних намірів. Умовно, за характером контенту, їх можна поділити на: **захисні**, **нейтральні** та **атакуючі**.

Проєкти, що містять інформацію, спрямовану проти конкретного супротивника, у вигляді прямих звинувачень, викриття, попередження, пошуку винних, відносяться до категорії з умовною назвою «захищаючі». Незважаючи на їх агресивний характер, вони використовуються переважно з метою оберігання − створення тимчасового або постійного ментального бар'єру в свідомості «своїх» цільових груп (мал. 5.5.). Також за допомогою таких проєктів можна частково здійснювати вплив на представників цільових груп, що не визначилися, або нейтральні по відношенню до певного системного конфлікту (міждержавний внутрішньодержавний), чи певної конфліктної ситуації.

*Мал.5.5.***«Захисні» мережеві проекти**



Мета захисних проєктів – підготовка цільових груп до можливих негативних ситуацій, викликання певних емоційних станів(позитивні або негативні), внесення легких психологічних установок на свідомому та підсвідомому розумовому рівні.

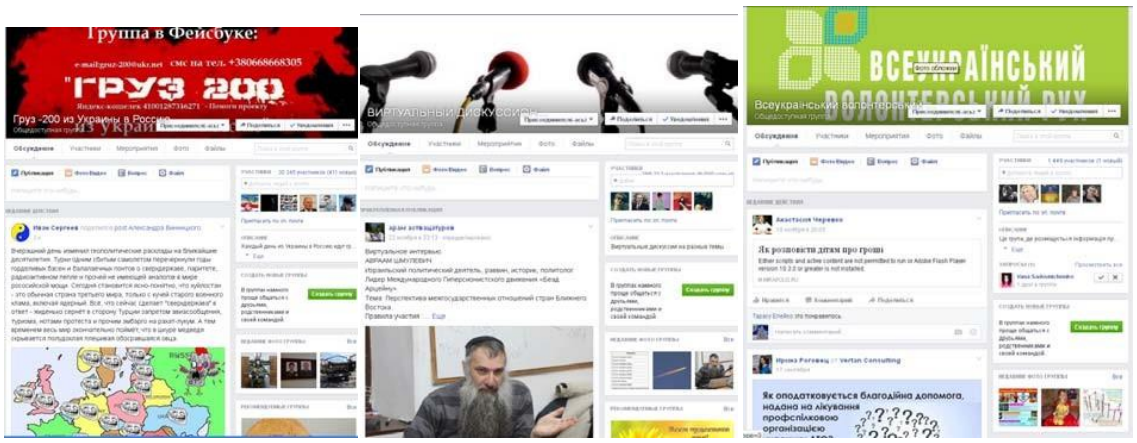
Зазначені проєкти використовуються в рамках реалізації таких стратегій, як консолідація та заспокоєння. В тактичному плані це робота переважно на власних майданчиках.

Мережеві проєкти, що містять інформацію про зміст та перебіг основних моментів конфліктів, без чітко визначених установок із зміщеними чи прихованими акцентами, маючи менш агресивний або взагалі нейтральний вигляд, насправді мають доволі потужний атакуючий потенціал.

Мета таких проєктів – привертання уваги до конфлікту, викликання певних емоційних станів (позитивні або негативні), внесення певних легких психологічних установок на свідомому розумовому рівні.

Такі проєкти використовуються в рамках реалізації різних варіантів стратегій – консолідація, заспокоєння, залякування, невдоволення, протест. У

тактичному плані передбачається робота на власних майданчиках та використання чужих для промоції власних проєктів (мал. 5.6).



Мал.5.6.**«Нейтральні» мережеві проекти**

Мета атакуючих проєктів – поширення інформації з прихованими інформаційними меседжами, викликання переважно негативних емоційних станів (агресивність або депресія), внесення ґрунтовних та легких психологічних установок на підсвідомому рівні (мал. 5.7).

Такі проєкти допомагають у реалізації стратегій, спрямованих на залякування, викликання невдоволення, дії протесту. В тактичному плані це може бути робота на власному майданчику, як опорному з акцентом на посіви на чужі майданчики.

Мал.5.7.**«Атакуючі»мережеві проекти**

Методи та засоби управління проєктами

Слід зазначити, що специфіка та особливості інтернет-технології web 2.0та 3.0 дають можливість певним чином корегувати систему управління проектами. Кожен такий проект створює власну, локальну мережу фоловерів, яка керується за відповідною схемою, що продиктована метою, завданнями та особливостями комунікаційної ситуації.

Найбільш зручною типологією для визначення таких систем є класифікація типів соціальних оф-лайн мереж, яка існує в системі розбудови оф-лайн соціальних мереж, а саме в Networking.

Відповідно до характеру або особливостей створення мережі в Networking визначається чотири базових типи: **променева**, **павуччя**, **3D** та **мисливська** [217, с.141-142].

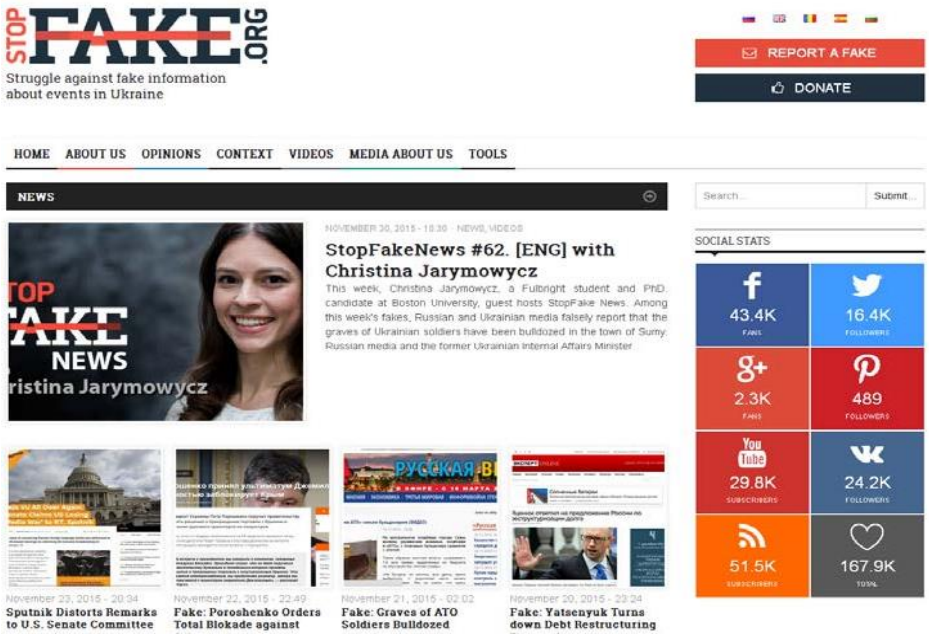
Променева мережа – структура, яка має центральну одиницю (особа або організація), об'єднує інших членів мережі, що не мають між собою контактів. Центральна одиниця є точкою, через яку здійснюються всі контакти. Така модель активно використовується в MLM і є типовою мережею із розповсюдження товарів та послуг (Oriflaime, Mary Kay, Amway та ін.).

Практичний приклад

В якості наочного прикладу проєкту, створеного на базових принципах променевої мережі, для ведення інформаційної війни можна навести інтернет-проект «StopFAKE».

Цей проєкт створено з метою виявлення та викриття неправдивої інформації, яку поширюють російські ЗМІ та структури, що практикують мережевий тролінг. В основі системи управління проєктом принцип радіального розповсюдження інформації з єдиного центру, яким є портал www.stopfake.org.

Базовий майданчик доповнюють групи в провідних соціальних мережах: Facebook (43,4 тис. фоловерів), VKontakte (24,2 тис. фоловерів), Twitter (16,4 тис. фоловерів), Google+ (2,3 тис. фоловерів), RSS. Останні використовують виключно з метою поширення інформації та посилення надійного ефекту від повідомлень.



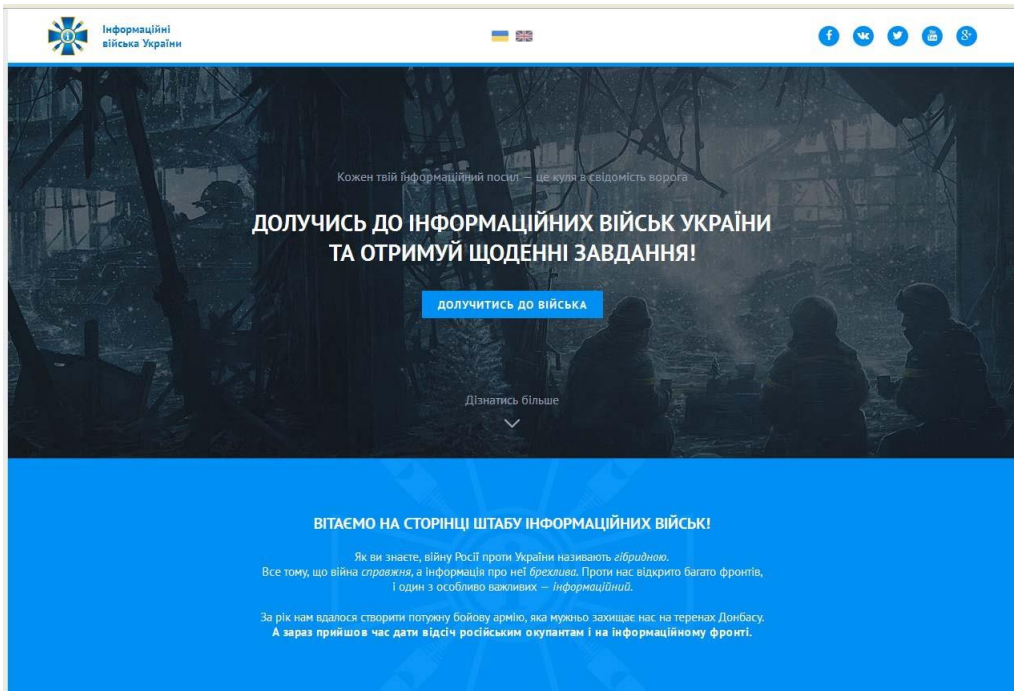
Павуччя мережа – структура спільноти, що передбачає можливість контактів між усіма членами мережі, в разі збереження координуючої функції її засновника – центральної одиниці. За такої моделі діють мережеві рекламні та консалтингові агенції, структури, що працюють за франшизою та ін. У рамках інформаційної війни така технологія управління є найбільш характерна для відкритих мережевих товариств – переважно мережевих тематичних груп, які ґрунтуються навколо одного сайту.

В такому разі сайт виконує функції координуючого центру, а безпосередньо контакти та спілкування відбуваються в мережевих групах.

Практичний приклад

В якості практичного прикладу проекту, в основі якого закладено зазначений принцип, можна навести «Інформаційні війська України».

Зазначений проєкт, створений в лютому 2015 р. Міністерством інформаційної політики України, в якості інструмента здійснення відповіді на російську інформаційну агресію.

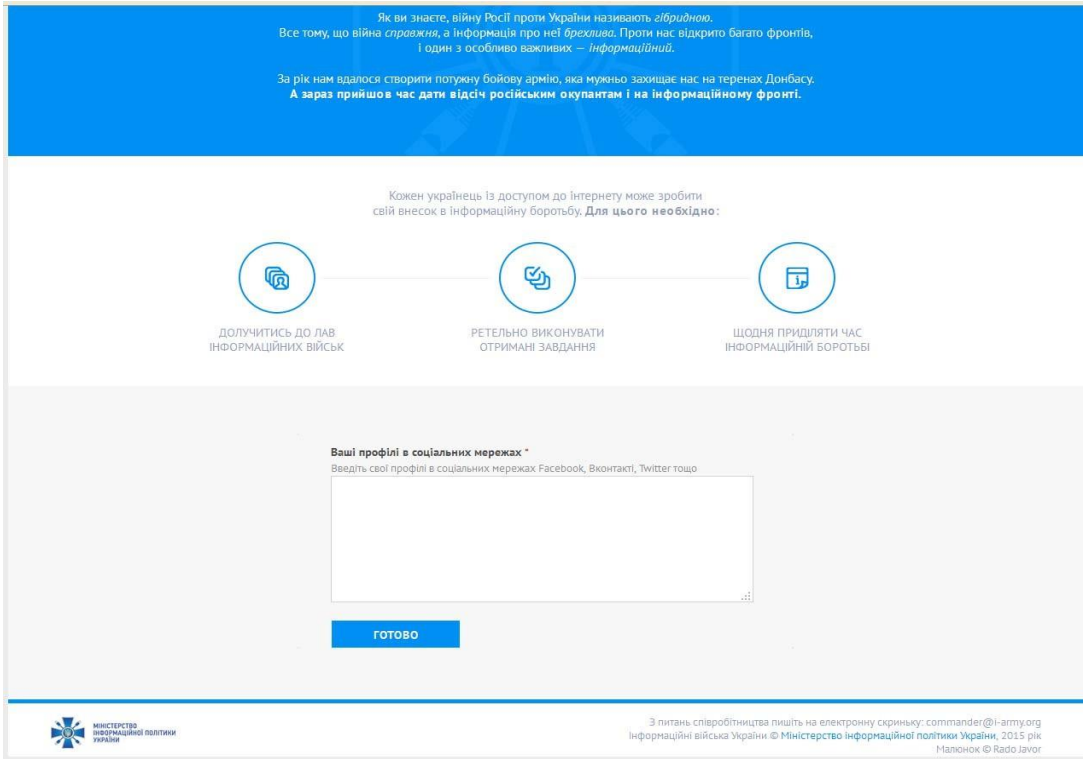


http://3.i-army.org/

Принцип та система управління проектом передбачає координацію кіберволонтерів із поширення певної інформації та збирання контенту, який може знаходитися в сфері інтересів проєкту.

На перших етапах існування даного проекту він в цілому відповідав принципам променевої мережі. З часом, у процесі трансформації, він набув рис саме павучої мережі, створивши тим самим систему більш гнучкою та відкритою для ефективних комунікацій.

Для того, щоб долучитися до проекту, необхідно пройти процедуру реєстрації, яка передбачає заповнення блоку питань – адреса електронної пошти, персональні профілі. На основі цієї інформації претендента включають у поштову розсилку новин та приєднують до груп «Інформаційних військ» у тих соціальних мережах, де претендент має персональні акаунти.



http://3.i-army.org/

Серед інформації, яка поширюється в рамках проекту, є репости цікавих матеріалів та власний контент (тексти, інфографіка, відео, меми). Відповідні матеріали доповнюються коментарями від модераторів проекту, які містять певні меседжі та психологічні установки.

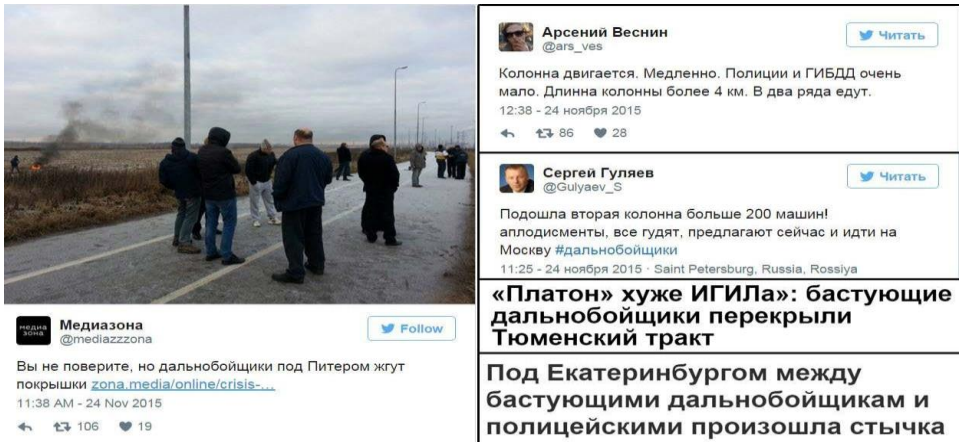
До контенту власного виробництва проекту можна віднести порівняльний моніторинг – подання різних поглядів на певні події з позиції, російських ЗМІ, європейських та українських.

Також активно поширюються матеріали із розвінчання російських фейків, на конкретних прикладах, з посиланнями й відповідною доказовою базою. В якості базового прийому, в такому разі, застосовується порівняння між автентичними матеріалами та підробленими.

Крім того, використовуються твіти або цитати лідерів громадської думки з приводу різноманітних подій для конкретизації певної позиції або тези, яку промотіюють модератори проєкту.

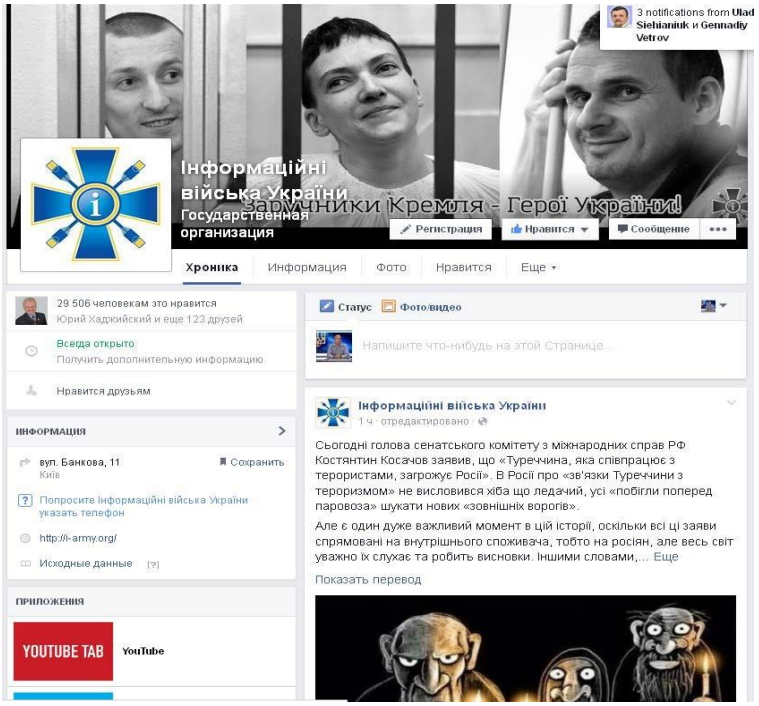
На початку існування проект мав значну підтримку серед представників патріотично налаштованого мережевого суспільства, втім останнім часом він втрачає популярність як через відсутність сенсаційних інформаційних приводів, так і через пасивність адміністраторів та модераторів проекту.

Вочевидь падіння популярності ресурсу є наслідком директивного та певною мірою примусового характеру комунікаційної схеми, яку пропонують адміністратори проекту. За умовами співпраці, кожен фоловер має поширювати контент, що продукується в рамках проекту. А також від учасників вимагається здійснювати моніторингові дії щодо інформаційного простору, до якого вони мають відношення.



У процесі роботи учасники проекту отримують інформацію на пошту та на інформаційні стрічки у соціальних мережах. Ця інформація має бути поширена в групах, в яких зареєстрований учасник та на особистому акаунті.

У рамках проекту функціонують групи та тематичні сторінки у таких соціальних мережах як: Facebook, VKontakte,Twitter,Google+,YouTube.

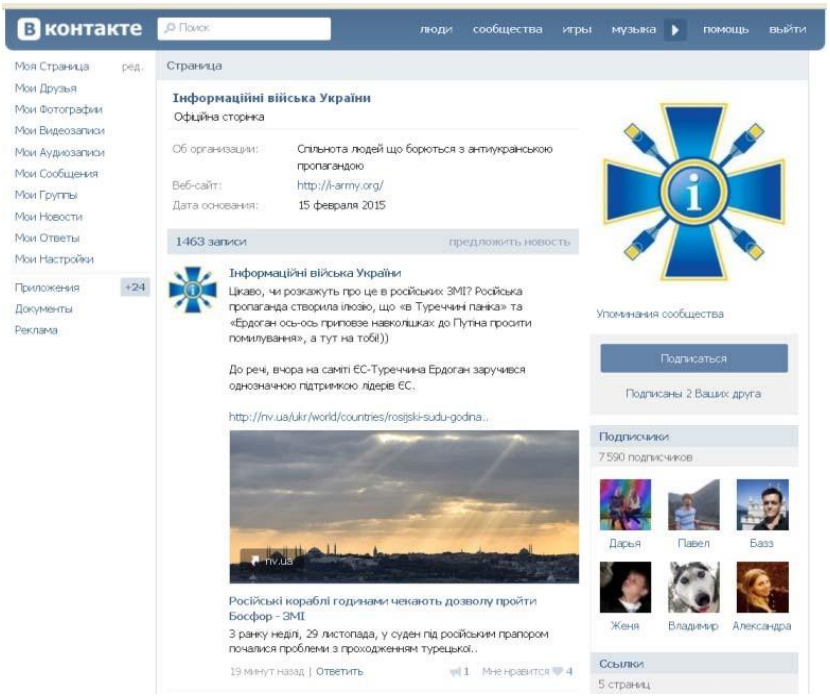


Сторінка проєкту у Facebook налічує зараз майже 30 тис. фоловерів. На сторінці фоловери можуть ставити лайки, коментувати, робити репост матеріалів. Також передбачена функція залишення повідомлень для інших фоловерів та модераторів сторінки.

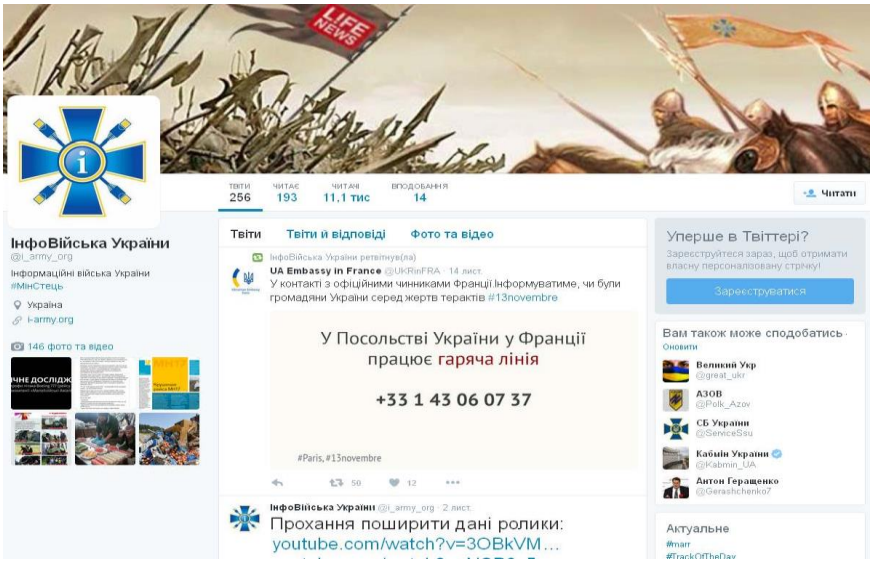
Пости на сторінці набирають у середньому від 10 до 100 лайків, найбільш популярні матеріали можуть отримувати до 500 лайків. Кількість репостів коливається в середньому 20-30, найбільш рейтингові матеріали можуть давати кілька сот репостів. Коментарів під цікавими публікаціями може нараховуватися 2-5. Популярні матеріали можуть зібрати кілька десятків коментарів. Останнім часом спостерігається падіння популярності групи проекту у Fecbook так само, як і проекту в цілому.

У соціальній мережі VKontakte нараховується близько 8 тис фоловерів, а сам майданчик має статус офіційної сторінки або закритої тематичної групи з можливістю пропонувати власні новини на розгляд модераторів.

Активність відвідувачів та фоловерів групи дає в середньому 5-15 лайків, 5-10 репостів та кілька коментарів під цікавими матеріалами. Резонансні матеріали можуть мати до 60-70 лайків, відповідно 20-30 репостів та до десятка коментарів.



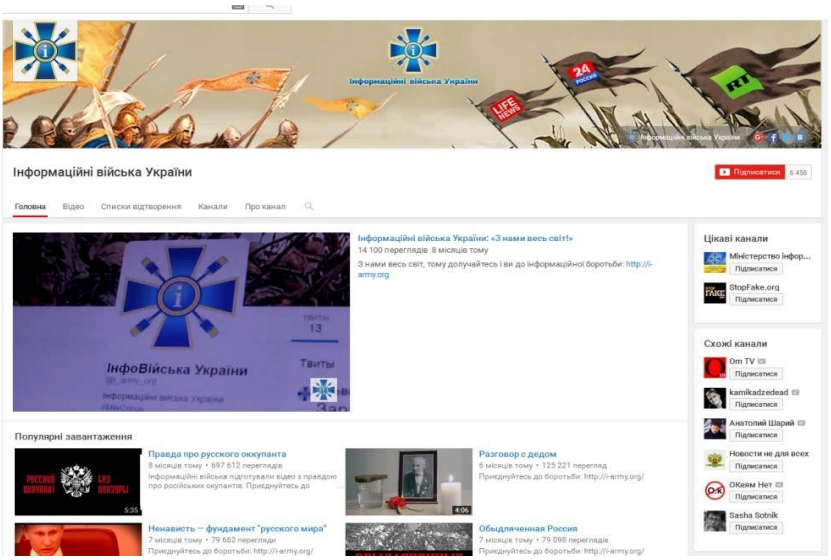
Так само, як і у випадку із попередньою соціальною мережею в сторінці проекту в VKontakte, останнім часом спостерігається значне падіння активності. На кількісні показники сторінки також впливає той факт, що зазначена мережа знаходиться під контролем відповідних російських структур.



У мережі Twitter сторінка проекту нараховує 11,1 тис фоловерів, регулярно знайомляться з твітами близько 200 фоловерів, в цілому створено близько 300 твітів. В середньому кожний більш-менш значущий твіт має 5-15

лайків та до 10 ретвітів. Важливі матеріали можуть назбирати 100-150 лайків та до сотні ревітів.

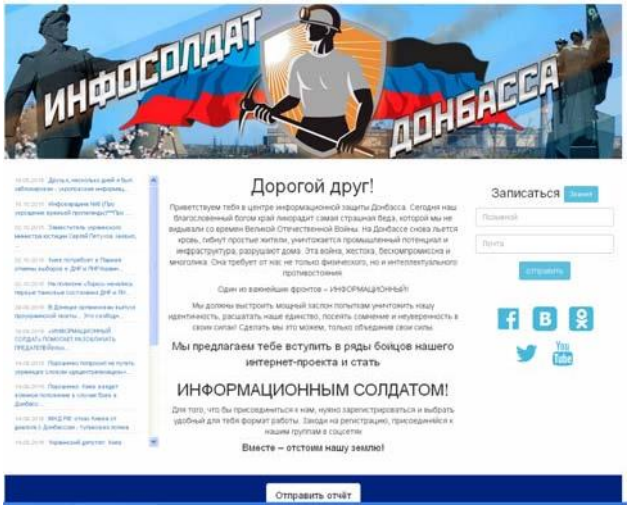
Слід зазначити, що модератори акаунту та адміністратори проекту «Інформаційні війська» не в повній мірі використовують усі можливості цієї соціальної мережі, що й позначається на результативності. Зокрема, абсолютно не використовується можливість миттєвого поширення новин або анонсів, зважаючи на достатньо значний потенціал.

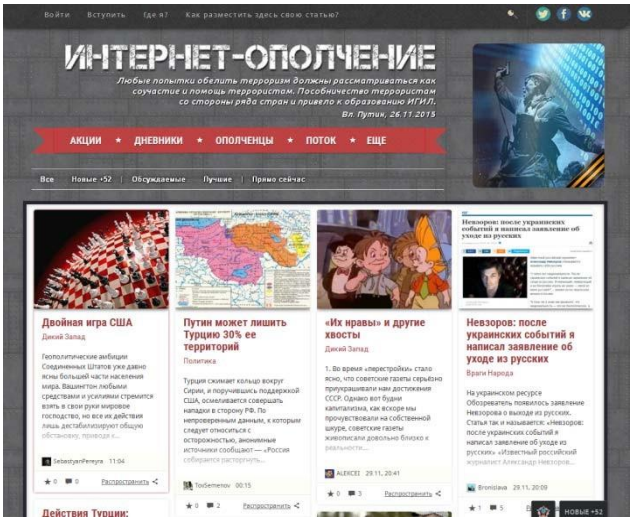


У соціальній мережі YouTube канал проекту «Інформаційні війська» нараховує майже 6,5 тис фоловерів, загальна кількість переглядів усіх матеріалів 1,14 млн на кілька десятків розміщених матеріалів.

Акаунт у соціальній мережі Google+має 1,3 тис фоловерів та є одним з найменш розвинутих в усьому проекті. Матеріали розміщуються нерегулярно і рідко. Відповідно реакція фоловерів на такі матеріали досить слабенька.

Серед проектів, подібних до «Інформаційних військ України», що діють в рамках інформаційної війни, російська сторона використовує низку централізованих (під контролем держструктур) тагромадських проектів. Останні мають різноманітне спрямування – в цілому по Україні («Интернет ополчение», «Киберберкут», «Антимайдан») або на окремі регіони («Информационный солдат Донбасса»).



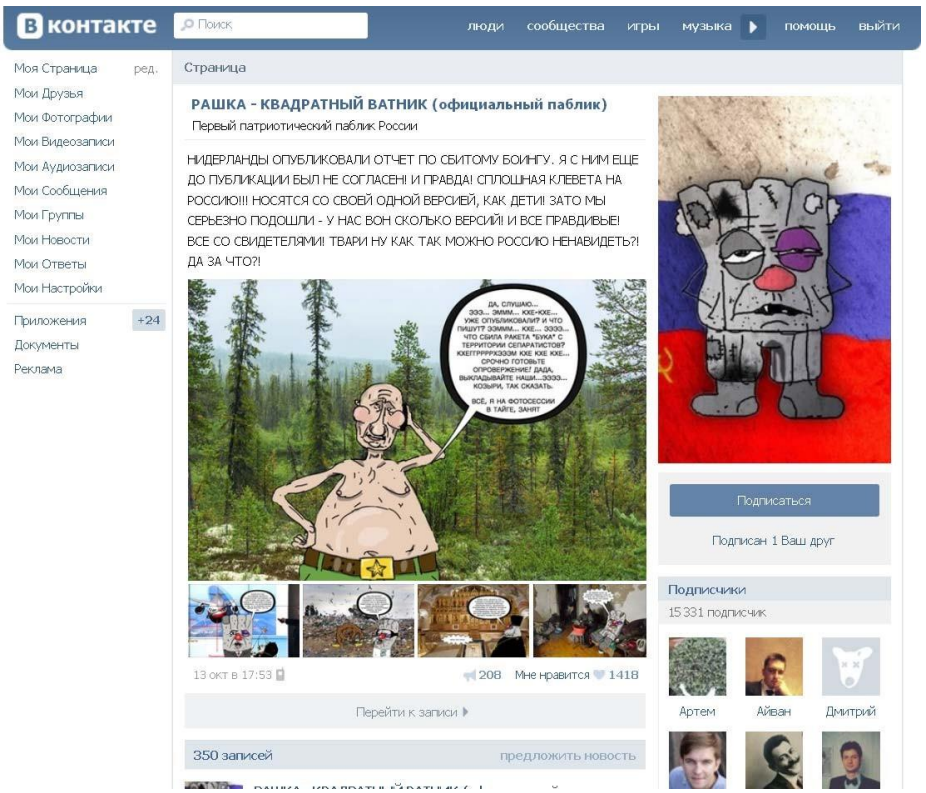


3D-мережа – об'єднання незалежних учасників, взаємодію яких регулюють принципи доцільності та корисності співпраці в межах даноїмережі. Єдиного координаційного центру не існує.

Практичний приклад

Практичний приклад проєкту, який функціонує за зазначеною схемою – офіційний паблік мережі VKontakte – «Ватник». Проєкт починався зі звичайного інтернет-мему і перетворився на знаковий в зв'язку із подіями 2014- 2015 рр. в Криму та на Сході України і в цілому в рамках російсько-української інформаційної війни.

На теперішній момент паблік нараховує 15,3 тис фоловерів. У середньому кожний матеріал має 100-200лайків, 20-30 репостів, кілька десятків коментарів. Найбільш популярні пости збирають 500-800 лайків, 100-150 репостів та до сотні коментарів.



http://vk.com/public_rushka

В якості контенту використовуються посилання на статті, відеоматеріали, меми, лоли, інфографіку. В рамках дискусій, у коментарях іноді застосовується ненормативна лексика, специфічні формати дискусії та інші форми спілкування, які забороняються та контролюються в переважній більшості подібних суспільств.

Система управління зазначеним проектом передбачає головного адміністратора (Антон Чадський) та чотирьох модераторів, які разом здійснюють наповнення контентом паблік і відповідно корегують політику проєкту.

У часи найбільшої активності даний паблік змінив систему координації з променевої на павуччю і на теперішній момент поповнюється контентом фактично за рахунок фоловерів, існуючих на доволі демократичних засадах.

Мисливська мережа – мережа, що утворюється внаслідок реструктуризації великих утворень шляхом розподілу на окремі юридично незалежні структури. Зазвичай таким шляхом йдуть потужні холдинги в тому разі, коли кон'юнктура передбачає більшу ефективність у діяльності дрібних компаній, які здатні гнучко реагувати на економічні виклики та налаштовуватися під нові ринкові умови.

Практичний приклад

В якості прикладу інтернет-проєкту, в системі координації якого закладається принцип мисливської соціальної мережі, – структура, яка спеціалізується на тролінгу. Зазвичай її називають «Ольгінка» або офіційно «Агентство интернет-исследований»[111].

Зазначена структура не є публічною, втім, аналізуючи систему та принципи розбудови управлінських принципів, вдалось встановити її базову схему роботи.

Основна робоча структура складається з великої кількості автономних блогерів, які обслуговують велику кількість персональних фейкових акаунтів (до 50 на одного троля). Тактика роботи передбачає кілька режимів:

- *режим вільного пошуку – моніторинг визначеної дільниці віртуального простору з метою відстеження ситуації, появи нових проектів, лідерів, ідейта меседжів;*
- *режим концентрованої атаки – об'єднання атакуючого потенціалу в коментарях під конкретним матеріалом в інтернет-виданнях або під постами в соціальних мережах;*
- *режим персонального контролю – спостерігання та помірковане участь у дискусіях по конкретному об'єкту (блог або акаунт).*

Принцип управління такими проектами передбачає створення певних координаторських одиниць, навколо яких гуртуються інші тролі.

Також в якості робочих одиниць можуть виступати окремі інтернет-проекти або групи із вузько спеціалізованим профілем. Зазвичай це може бути регіональний або тематичний принцип.

Медіа-віруси та їх використання в якості інформаційної зброї

Будь-яка ефективна інформаційна атака починається з латентної фази – прихованого проникнення в інформаційне поле противника з метою дослідження середовища, апробації певних ідей та потенційного ефекту їх застосування, а також для створення і закріплення власних інформаційних майданчиків для подальшої агресії.

Найкращим інструментом для проникнення на вороже інформаційне поле є так званні **медіа-віруси** – інформаційні носії (події, скандали, чутки, діяльність організацій та окремих осіб), що несуть у прихованому вигляді завуальовані ідеї та меседжі.

Зазвичай медіа-віруси можуть поширюватися у вигляді мемів та лолів– окремих семіотичних фрагментів[185].

Д.Рашкофф визначає декілька типів медіа-вірусів, серед яких[351,с.124]:

1. ***Цілеспрямовані віруси*** - реклама, передвиборчі гасла, штучно детоновані «інформаційні бомби».
2. ***Віруси-тягачі***- спонтанно виникають та миттєво підхоплюються, а також наповнюються певним змістом, що спрямований на вирішення певних завдань.
3. ***Спонтанні віруси*** – народжуються та поширюються без конкретної цілі, в разі успішності можуть бути використані для вирішення певних завдань.

Найбільш вдалою формою камуфляжу для медіа-вірусів є події, винаходи, інноваційні технології, наукові теорії, філософські системи та культурологічні концепції. Саме за допомогою таких форматів простіше всього здійснювати проникнення в певне інформаційне середовище, не викликаючи особливих підозр.

У рамках еволюції медіа-вірусів з'явилося таке явище, як **медіа-активізм**– тактика партизанської інформаційної війни, що реалізується окремими медіа-активістами або групами таких активістів.

Тактика медіа-активізму передбачає створення певних розкручених персон або організацій (рухів, громадських ініціатив та ін.), які є авторами та трансляторами тематичних медіа-вірусів.

В онлайн соціальних мережах до медіа-активістів можна віднести тематичні групи або окремих блогерів, які виконують функції своєрідних кібер-диверсантів.

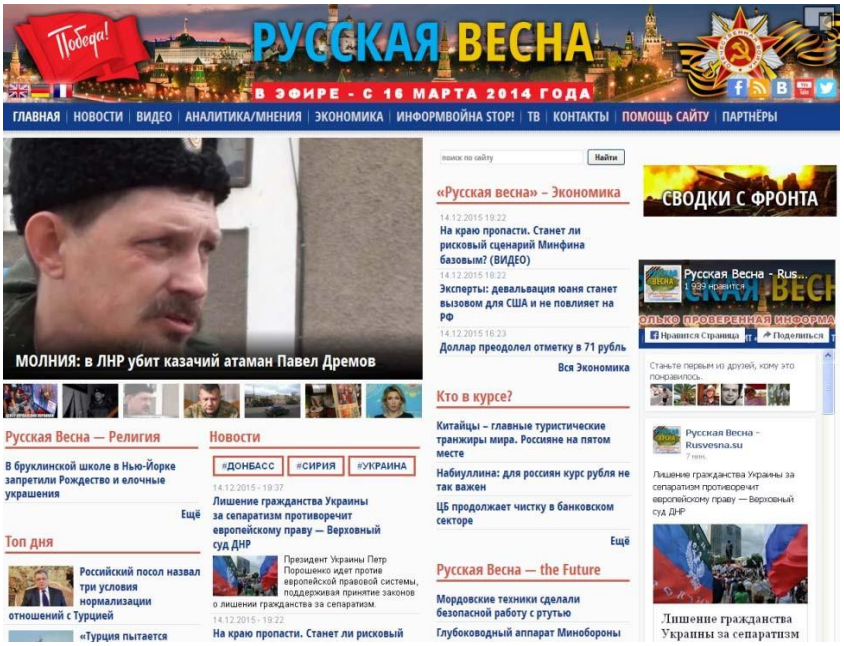
Особливо активно ця технологія застосовувалася в піковий період російської агресії в Криму та східних регіонах України.

До кола таких товариств можна віднести низку груп під загальним брендом «Антимайдан», «КиберБеркут»,«Интернет-ополчение» та ін.

Мал.5.8.**Медіа-активіські рухи**

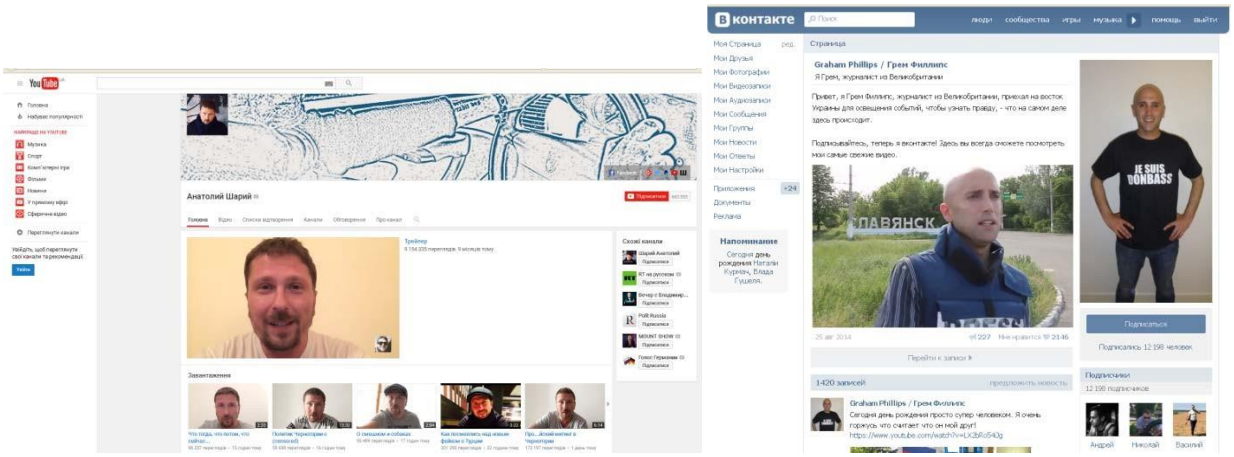
Також достатньо відомим трендовим медіа-вірусом став інтернет проект «Русская весна», який є уособленням та головною ідеологічною платформою російською агресії в Україні.

Мал.5.9.**Медіа-вірус «Русская весна»**



Серед персоналій, яких можна вважати медіа-активістами, стали Анатолій Шарій, Грем Філліпс, Ігор Стрєлков та інші відомі медіа-персонажі, які уособлюються із інформаційно-психологічною війною, що супроводжувала російську агресію в Криму та на Сході України в 2014-2015 рр.

Мал.5.10.**Медіа-активістивросійсько-українськийвійні(2004-2015рр.)**



В якості прикладу медіа-вірусів подій можна навести прес-конференції екс-президента України В.Януковича в Ростові. Мета цієї інформаційної атаки - сприяння розколу в українському суспільстві, підбурення лояльних до президента-втікача проти офіційної української влади, яка отримала мандат Майдану.

Мал.5.11.**Медіа-вірус «Прес-конференція В. Януковича в Ростові»**

Серед останніх найбільш гучних медіа-вірусів скандалів можна визначити звинувачення російських медіа прем'єр-міністра України щодо його участі в чеченській війні. Абсурдність звинувачення була очевидною з самого початку і саме цей медіа-вірус носив характер фарсу.

Мал.5.12.**Медіа-вірус «Яценюк в Чечні»**

Також можна визначити медіа-віруси як інструменти інформаційно-психологічних атак, які за сутністю є поліваріативними та носять у собі класичні ознаки інформаційної війни другого покоління із елементами асиметрії. За своїми базовими ознаками та характеристиками вони відповідають визначенню інформаційної зброї.

Разом з наочними перевагами медіа-вірусів необхідно зазначити й певні технологічні недоліки, які виходять, перш за все, з суб'єктивного характеру цього явища. Сприйняття, підтримка або ігнорування такого інформаційного повідомлення цілком залежить від персональної реакції кожного конкретного отримувача.

Також слід зазначити, що вірусний характер контенту в соціальних он-лайн мережах може бути неконтрольований. Вдалий медіа-вірус, який отримує масову підтримку користувачів, починає існувати за законами та принципами притаманними внутрішньо груповій комунікації. Крім того, в певних ситуаціях його рух здійснюється за принципами та механізмами ройового інтелекту, який спрацьовує як засіб саморегулювання інформаційних потоків у певних соціальних суспільствах, до яких також відносяться і соціальні онлайн мережі.

ВИСНОВКИ

У системі сучасних економічних, політичних та військових протистоянь інформаційні війни в соціальних онлайн мережах посідають провідне місце, як один з ключових супроводжувальних процесів. Головне призначення таких процесів – шляхом концентрації зусиль на певних ключових ланках, забезпечувати суттєві переваги в рамках комплексного протиборства сторін. Інформаційна зброя такого типу здатна знищувати чи, як мінімум, блокувати системи координації, поширення інформації та інші відповідні управлінські процеси, а також перешкоджати роботі відповідних центрів керування. Спектр інструментів при цьому доволі широкий – від кібератак до організації акцій протесту, терористичних актів та організованого збройного опору.

Інформаційно-психологічні операції є сьогодні невід'ємною частиною систем управління військами, політичними та економічними процесами. У зв'язку з активною віртуалізацією людства, такі конфлікти переносяться у інтернет-простір і набувають формату мережевих онлайн протистоянь.

Останнє викликає необхідність налагодження системної роботи за двома напрямками. Перший – розробка та впровадження стандартів і алгоритмів ведення мережевих інформаційних війн, які допомагатимуть швидко реагувати на певні виклики та компенсувати в певних обставинах відсутність досвіду та власних інструментів. Другий напрямок – налагодження системної роботи із підготовки відповідних фахівців, що спиратиметься на чітку методологічну базу та практичні методики навчання.

Важливість роботи за двома зазначеними вище напрямками полягає втому, що інформаційні війни, на відміну від торгово-економічних, політичних та збройних протистоянь, ніколи не закінчуються. Тому питання державної інформаційної безпеки в зазначеному контексті є завжди актуальним.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Нормативно-правова база

1. Конституція України [Текст]: прийнята на п’ятій сесії Верховної Ради України 28 червня 1996 р. *Відом. Верхов. Ради України.* 1996. №30.
2. Закон України «Про інформацію» [Текст] *Інформаційне законодавство:* збірник законодавчих актів у 6 томах / за ред. Ю.С. Шемшученка.Т.1*Інформаційне законодавство України.* Київ: ТОВ «Юридичнадумка»,2005. С.9-28.
3. Про друковані засоби масової інформації (пресу) в Україні [Текст]: Закон України. *Інформаційне законодавство:* збірник законодавчих актів у 6 томах / за ред. Ю.С. Шемшученка. Т.1Інформаційнезаконодавство України. Київ: ТОВ «Юридична думка», 2005. С. 29-43.
4. Про телебачення та радіомовлення [Текст]: Закон України. *Інформаційне законодавство:* збірник законодавчих актів у 6 томах / за ред. Ю.С. Шемшученка.Т.1.-*ІнформаційнезаконодавствоУкраїни.* Київ: ТОВ «Юридичнадумка»,2005.С.44-69.
5. Про інформаційні агентства [Текст]: Закон України. Інформаційне законодавство: збірник законодавчих актів у 6 томах / за ред. Ю.С.Шемшученка.– Т.1.ІнформаційнезаконодавствоУкраїни. Київ: ТОВ «Юридичнадумка»,2005. С.73-82.
6. Про рекламу [Текст]: Закон України. *Інформаційне законодавство*: збірник законодавчих актів у 6 томах / за ред. Ю.С. Шемшученка. Т.1ІнформаційнезаконодавствоУкраїни. Київ:ТОВ «Юридичнадумка»,2005.С.106-123
7. Про телекомунікації [Текст]: Закон України. *Інформаційне законодавство*: збірник законодавчих актів у 6 томах / за ред. Ю.С. Шемшученка.Т.1ІнформаційнезаконодавствоУкраїни.Київ:ТОВ «Юридичнадумка»,2005.С.124-165.
8. Про порядок висвітлення діяльності органів державної влади та місцевого самоврядування в Україні засобами масової інформації [Текст]: Закон України. *Інформаційне законодавство:* збірник законодавчих актів у 6 томах / за ред. Ю.С. Шемшученка. Т.1Інформаційне законодавство України. Київ: ТОВ «Юридична думка», 2005. С. 166-176
9. Про захист персональних даних: Закон України . *Верховна Рада України:* [сайт].URL: http://zakon3.rada.gov.ua/laws/show/2297-17
10. Про видавничу справу: Закон України. *Інформаційне законодавство:* збірник законодавчих актів у 6 томах / за ред. Ю.С. Шемшученка. Т.1ІнформаційнезаконодавствоУкраїни. Київ: ТОВ «Юридичнадумка»,2005. С.234-247.
11. Про державну таємницю: Закон України. *Інформаційне законодавство:* збірник законодавчих актів у 6 томах / за ред. Ю.С. Шемшученка. Т.1 *Інформаційне законодавство України.* Київ: ТОВ «Юридичнадумка»,2005. С.252-276
12. Про захист інформації в авторизованих системах: Закон України. *Інформаційне законодавство:* збірник законодавчих актів у 6 томах / за ред. Ю.С.Шемшученка. Т.1.-Інформаційне законодавство України. Київ: ТОВ «Юридичнадумка»,2005. С.277-282
13. Про доступ до публічної інформації: Закон України. *Верховна Рада України:* [сайт]. URL: http://zakon0.rada.gov.ua/laws/show/2939-17
14. Про державну службу спеціального зв’язку та захисту Інформації України: Закон України *Верховна Рада України*: [сайт]. URL: http://zakon0.rada.gov.ua/laws/show/3475-15

15. Про наукову та науково-технічну експертизу. *Верховна Рада України*: [сайт] URL: http://zakon1.rada.gov.ua/laws/show/51/95-%D0%B2%D1%80
16. Про електронні документи та електронний документообіг: Закон України. *Верховна Рада України*: [сайт]. URL: http://zakon5.rada.gov.ua/laws/show/851-15
17. Про засади державної мовної політики: Закон України. *Верховна Рада України* [сайт]. URL: http://zakon3.rada.gov.ua/laws/show/5029-17.

Наукові та науково-прикладні статті і видання

1. Ананьїн В., Пучков О. Інформаційна безпека у контексті сучасних подій в Україні [Текст]. *Вісник Київського національного університету імені Тараса Шевченка*. 2007. № 14-15. С. 28–29.
2. Андреєва О.М. Національна безпека України в контексті національної ідентичності і взаємовідносин з Росією [Текст]. Київ: Парламентське видавництво, 2009. 360 с.
3. Бабіч О. Особливості маніпуляції масовою свідомістю в друкованих ЗМІ під час висвітлення воєнних подій [Текст]. *Вісник Київського національного університету імені Тараса Шевченка:* військово-спеціальні науки. 2007. Вип. 14 – 15. С. 89–92.
4. Бажан О. Г. Українська Гельсінська група: легальна форма протистояння тоталітарному режимові в УРСР [Текст]. Національний ун-т «Києво-Могилянська академія». Наукові записки. Київ, 1999. Т.14: Історія. С.73–79.
5. Вєдєнєєв Д.В. Гострі когті орла. Сили спеціальних операцій США: історія та сучасність [Текст]: монографія / Д.В. Вєдєнєєв, Г.С. Биструхін, А.І.Семука. Київ: К.І.С., 2010. 400 с.
6. Вєдєнєєв Д.В. «Міжнародний тероризм» : цілісне явище модерної військової історії чи пропагандиський штамп [Текст]. *Труди Національного університету оборони України*. 2009. №2. С.186-192.
7. Вишняков О. Інформаційна війна з Росією: уроки виживання. ICTV: [сайт]. URL: fakty.ictv.ua/index/read-blog/id/1713.
8. Волович О. Інформаційно-психологічні операції США в Іраку [Текст]. *Ірак на шляху випробувань і відродження.* Одеса: Фенікс, 2010. С. 114–126.
9. Галака О. Основні тенденції розвитку та ймовірні форми воєн та збройних конфліктів майбутнього [Текст] / О.Галака, О.Ільяшов, Ю.Павлюк. *Наука і оборона.* 2007. №4. С.10-15.
10. Домарев В.В. Інформаційна зброя: принципи дії та основні види. *Секьюрити:* [сайт]. URL: http://www.security.ukrnet.net/modules/sections/index.php?op=viewarticle&artid=729.
11. Дергачов О.П. Партнерський потенціал України: становлення і реалізація [Текст]. Київ: Парламентське видавництво, 2009. 496 с.
12. Зеленін В.В. Сучасні агітаційно-пропагандистські технології в регіональних виборчих кампаніях: *дайджест навчально-методичних рекомендацій* [Текст]. Київ: ЦСВТ, 2013. 116 с.
13. Казакова О.М. Політика нацистської Німеччини щодо населення окупованих польських територій 1939 – 1941 рр. [Текст]. *Культурологічний вісник:* науково-теоретичний щорічник Нижньої Наддніпрянщини. 2007. Випуск 18.С. 41–44.
14. Квіт С. Масові комунікації [Текст]: підручник. Київ: видавничий дім «Коєво-Могилянська академія», 2008. 206 с.
15. Телебачення спецопераций [Текст] /Н.Лігачова, С.Черненко, В.Іванов. Київ:ТелеКритика,2003. 266с.

16. Литвиненко О. Інформаційний простір та його захист: теорія і практика [Текст]. *Віче*. Київ, 2000. № 10. С. 119–127.
17. Литвиненко О.В. Інформаційний вплив та операції: теоретико- аналітичні нариси: *монографія* [Текст]. Київ: НІСД, 2003. 240 с.
18. Радковець Ю. Гібридна політика сучасної Росії. *Урядовий кур'єр* [сайт]. 2015. 20 жовтня. URL: http://ukurier.gov.ua/uk/articles/gibridna-politika-suchasnoyi-rosiyi/
19. Сватко Я. Національна безпека України в умовах ведення інформаційних. Західна аналітична група [сайт]. URL: http://zgroup.com.ua/print.php?articleid=1606.
20. Слюсаренко А. В. Особливості проведення психологічних операцій в зоні перської затоки (1990-1991) та в Іраку (2003) [Текст] Збірник наукових праць. Київ: Національна академія оборони України, 2004. С. 60–68.
21. Україна в сучасному геополітичному просторі: теоретичний і прикладний аспект [Текст]: монографія/ За ред. Ф.М.Рудича. Київ: МАУП, 2002. 488 с.

Видання підготовлено до друку та віддруковано
редакційно-видавничим відділом КНЗ «ЧОІПОПП ЧОР»
Зам. № 1720 Тираж 100 пр.
18003, Черкаси, вул. Бидгощська, 38/1