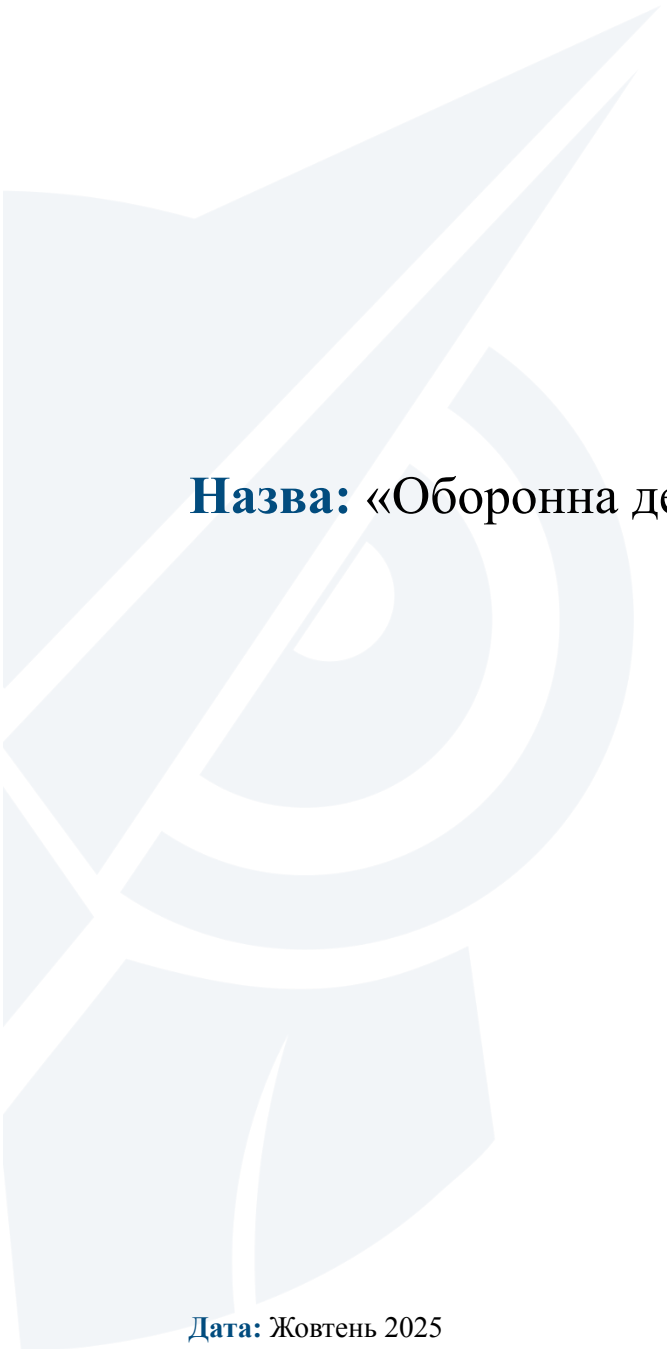




Назва: «Оборонна демократія в інформаційній сфері»

Дата: Жовтень 2025

Організація: ГО «Фонд сприяння демократії» за сприяння Фонду Ганнса Зайделя в Україні

Команда дослідників: Юрій Гончаренко, Ольга Максимова, Андрій Васильчук, Валерій Майданюк, Соломія Шваничик, Костянтин Канішев

Дисклеймер: Дослідження базується на аналізі відкритих джерел, експертного опитування та опитувань, проведених в межах роботи «**Українського безпекового клубу**». Думки й оцінки належать авторам і не обов'язково відображають офіційну позицію організацій-партнерів. Показники можуть змінюватися з розвитком подій.

РОЗДІЛ I. КОНЦЕПТУАЛЬНІ ЗАСАДИ

1.1. Визначення та еволюція концепту оборонної демократії

Оборонна демократія як цілісна концепція виникла завдяки зусиллям Українського безпекового клубу в 2025 році, представляючи собою унікальну українську розробку, що комплексно охоплює всі сфери суспільного життя, на відміну від попередніх фрагментарних підходів, які мали інші назви, були актуальними для інших епох та обмежувалися вузькими аспектами захисту демократичних інституцій. Ця ідея має коріння в історичних уроках криз XX століття, особливо – в досвіді Веймарської республіки, коли демократичні системи виявилися вразливими перед силами, що використовували їхні ж механізми для самознищення, перетворюючи толерантність на слабкість і вимагаючи активного самозахисту через правові інструменти, але саме український досвід гібридної війни надав концепції нового виміру та глибини.

З часом концепція еволюціонувала, охоплюючи не лише політичні загрози часів холодної війни, але й виклики тероризму 1970-2000-х років, падіння авторитарних режимів наприкінці XX століття та гібридні атаки в сучасності, де фокус зсувається від фізичного захисту інституцій до охорони цінностей і суспільної єдності, особливо в умовах, коли війна ведеться в онтологічному вимірі, атакуючи саму природу реальності, ідентичності та стабільності світу через маніпуляцію сприйняттям і колективною свідомістю.

У цифрову еру демократія змушена адаптуватися до нових реалій, коли загрози стають «невидимими» й маніпулятивними, перетворюючи інформаційний простір на головне поле битви, де використовуються соціальні мережі, алгоритми, боти та технології глибоких фейків. Які здатні розхитувати довіру до об'єктивної реальності ефективніше, ніж традиційна військова агресія, створюючи паралельні світи сприйняття, де факти втрачають значення, а емоції стають головним драйвером прийняття рішень. Ця адаптація передбачає створення проактивних систем, які не лише реагують на дезінформацію постфактум, але й запобігають їй через формування стійких смислових рамок, забезпечуючи складний баланс між захистом суспільства від маніпулятивних впливів та збереженням фундаментальної свободи слова, де плюралізм думок стає не слабкістю, а силою демократії в умовах постійних інформаційних атак.

В українському контексті потреба в цій концепції набула особливого екзистенційного значення, як інструмент виживання нації в період від Революції Гідності до повномасштабного вторгнення та подальшої Великої війни за Незалежність. Під час Майдану 2013-2014 років громадянське суспільство продемонструвало, як масова мобілізація сил та горизонтальні мережі довіри можуть ефективно протистояти централізованій пропаганді, викриваючи маніпуляції авторитарного режиму та формуючи альтернативні наративи свободи й гідності, але водночас цей період виявив системні прогалини в національній інформаційній обороні, особливо щодо протидії зовнішнім впливам. Після початку російської агресії 2014 року Україна почала вибудовувати власну модель інформаційної політики шляхом проб і помилок, від заборони російських телеканалів до створення інституцій стратегічних комунікацій, що стало адаптивною відповіддю на постійні атаки, спрямовані на розкол суспільства через експлуатацію регіональних, мовних та історичних відмінностей. Повномасштабне вторгнення 2022 року кардинально прискорило цей процес, перетворивши інформаційну сферу на критичний фронт виживання, де оборонна демократія (яка ще не отримала цю назву інституційно) органічно інтегрується з військовими зусиллями, дипломатією та економічною стійкістю. Де Україна активно ділиться унікальним досвідом протидії гібридним загрозам, включаючи онтологічні атаки на колективну ідентичність і фундаментальне сприйняття реальності.

1.2. Нормативно-етична рамка

Нормативно-етична основа оборонної демократії в інформаційній сфері глибоко корениться в християнсько-демократичних принципах, які ставлять людську гідність у центр будь-якої політики, перетворюючи протидію інформаційним загрозам на спільну справу всього суспільства, а не лише державних інституцій чи спеціальних служб. Персоналізм як філософська основа підкреслює, що кожна людина є не просто пасивним об'єктом маніпулятивних впливів чи статистичною одиницею в інформаційних потоках, а активним суб'єктом, наділеним розумом і здатним до критичного мислення та морального вибору, тому інформаційна оборона спрямована не на заміщення цієї здатності

державним патерналізмом, а на її систематичне посилення через освітні програми, технологічні інструменти самозахисту та створення середовища, де критичне мислення цінується й заохочується.

Солідарність трансформує боротьбу з дезінформацією з вузького завдання спецслужб чи медіарегуляторів на колективну відповідальність усього суспільства, де журналісти виступають першою лінією виявлення маніпуляцій, освітяни формують критичне мислення нових поколінь, релігійні лідери підтримують моральні орієнтири в хаосі інформаційних атак, а громадські активісти створюють горизонтальні мережі верифікації та взаємопідтримки, об'єднуючись у спільноту, де культура правди стає фундаментом суспільної єдності та стійкості проти розколу. Субсидиарність як організаційний принцип забезпечує ефективну децентралізацію інформаційної оборони, визнаючи, що локальні громади краще розуміють свої специфічні вразливості, культурні особливості та комунікаційні канали, тому можуть реагувати на локальні фейки та маніпуляції швидше й точніше, ніж централізована бюрократична машина, яка встановлює лише загальні правові та етичні рамки, не намагаючись монополізувати процес протидії дезінформації.

Баланс між національною безпекою та свободою слова стає центральним викликом оборонної демократії, де будь-які обмеження інформаційних свобод розглядаються виключно як *ultima ratio* - крайній засіб, що застосовується лише за наявності реальної, безпосередньої та серйозної загрози демократичному ладу чи національній безпеці, з обов'язковою відповідністю трьом критеріям: необхідності, коли загроза не може бути усунена іншими засобами; пропорційності, коли обмеження не перевищують масштабу загрози; та тимчасовості, з чітко визначеними умовами та термінами скасування обмежень, причому кожне таке рішення супроводжується детальним публічним обґрунтуванням та підлягає незалежному судовому контролю. Це створює систему, яка не придушує плюралістичну дискусію як основу демократії, а навпаки - формує умови для її здорового розвитку, де свобода слова не перетворюється на інструмент руйнування самої демократії.

Правові запобіжники та механізми контролю формують складну мережу стримувань і противаг, де незалежні органи медіарегулювання з обов'язковим громадським представництвом співпрацюють з регулярними парламентськими слуханнями щодо стану інформаційної безпеки, громадськими радами при органах стратегічних комунікацій забезпечують транспарентність процесів, а обов'язкові оцінки впливу на свободу слова проводяться для кожного обмежувального заходу, доповнюючись ефективними механізмами оскарження рішень та справедливої компенсації за помилкові обмеження, що робить всю систему гнучкою, адаптивною та підзвітною, запобігаючи як авторитарним зловживанням владою, так і анархічному хаосу нерегульованого інформаційного простору.

1.3. Теоретична модель інформаційної стійкості

Теоретична модель інформаційної стійкості вибудовується навколо чотирирівневої архітектури, де кожен структурний елемент органічно переходить у наступний, створюючи не лінійну послідовність, а динамічний замкнений цикл захисту та розвитку демократичного інформаційного простору. Перший стовп - моніторинг і раннє виявлення - починається з систематичного безперервного сканування всього спектру інформаційного простору через автоматизовані системи та експертний аналіз, виявляючи не лише окремі фейки, але й координовані кампанії дезінформації, аномальні патерни поширення контенту, ботомережі та інші ознаки маніпулятивного впливу, картографуючи еволюцію ворожих наративів від зародження до масового поширення та прогнозуючи майбутні інформаційні атаки на основі виявлених закономірностей, що дозволяє переходити від реактивного реагування до проактивного запобігання.

Другий стовп - стратегічні комунікації та швидка відповідь - трансформує дані моніторингу в скоординовану дію, де проактивне формування порядку денного через випереджувальні меседжі синхронізується між усіма державними та громадськими комунікаторами через єдину рамку ключових наративів, які водночас залишаються достатньо гнучкими для адаптації під специфіку різних цільових аудиторій, враховуючи їхні культурні коди, канали споживання інформації та психологічні особливості сприйняття, створюючи мультиканальну екосистему правдивої інформації, яка випереджає та нейтралізує дезінформаційні атаки через насичення інформаційного простору якісним контентом.

Третій стовп - стійкість громад і медіаграмотність - переносить фокус з централізованих зусиль на розвиток розподіленої мережі стійкості, де систематичний розвиток критичного мислення через формальну та неформальну освіту поєднується зі зміцненням локальних мереж довіри в громадах, створенням безпечних просторів для діалогу між різними соціальними групами, наданням психологічної підтримки в умовах інформаційного стресу та травматизації, формуванням глибоких культурних імунітетів проти маніпуляцій через відродження автентичних традицій, історичної пам'яті та ціннісних орієнтирів, що робить кожну громаду не пасивним об'єктом захисту, а активним суб'єктом інформаційної оборони.

Четвертий стовп - етика, право і прозорість - завершує архітектурну конструкцію, встановлюючи чіткі, зрозумілі та справедливі правила гри для всіх акторів інформаційного простору, від медіавласників до блогерів, включаючи обов'язкове розкриття реальних бенефіціарів медіа та джерел фінансування, впровадження та дотримання високих етичних стандартів журналістики через механізми саморегулювання та професійної відповідальності, забезпечення постійної підзвітності через регулярні публічні звіти, відкриті слухання та ефективні механізми громадського контролю, що створює середовище, де маніпулятивні практики стають не вигідними та соціально неприйнятними.

Ця модель нерозривно пов'язана з фундаментальною концепцією соціальної згуртованості та багаторівневої довіри, де інформаційна стійкість суспільства зростає не лінійно, а експоненційно пропорційно до рівня соціальної єдності, перетворюючи атомізоване, фрагментоване суспільство з низьким рівнем довіри - ідеальну мішень для дезінформаційних атак - на консолідовану спільноту з природним імунітетом проти маніпуляцій. Модель працює одночасно на трьох взаємопов'язаних рівнях довіри: горизонтальному, що формується між громадянами через спільний досвід, взаємодопомогу та солідарність; вертикальному, що вибудовується між громадянами та інституціями через прозорість, підзвітність та ефективність; та епістемологічному, що визначає довіру до джерел знання, експертизи та способів встановлення істини, створюючи синергетичний ефект взаємного підсилення. Проект INFOLIGHT.UA – 2025 втілює цю теоретичну модель у практичну площину, працюючи одночасно на всіх рівнях та створюючи мультиплікативний ефект для посилення національної резиліентності, особливо у протидії онтологічним загрозам, що атакують фундаментальні аспекти колективного існування, ідентичності та сприйняття реальності.

РОЗДІЛ II. АНАЛІЗ ЗАГРОЗ ТА ВИКЛИКІВ

2.1. Картографія інформаційних загроз

Системна російська дезінформація: методи та інструменти

Російська дезінформаційна машина представляє собою безпрецедентну за масштабом та складністю систему, яка еволюціонувала від радянської пропаганди до сучасної мультимедійної екосистеми маніпуляцій, інтегруючи традиційні медіа, цифрові платформи, дипломатичні канали та агентурні мережі в єдиний механізм, спрямований не просто на спотворення фактів, а на руйнування самої здатності розрізняти правду та брехню, реальність та фікцію. Ця система працює через координовані кампанії, де державні медіа типу RT та Sputnik створюють первинний контент, який потім підхоплюється мережею псевдонезалежних сайтів, телеграм-каналів та соціальних акаунтів, створюючи ілюзію множинності джерел та органічного поширення, при цьому використовуючи алгоритми платформ для максимізації охоплення та залучення через емоційно заряджений контент, що експлуатує страхи, упередження та травми цільових аудиторій. Вони не просто дезорієнтують окремих індивідів, а систематично розхитують фундаменти суспільства, підживлюючи внутрішні конфлікти, зневіру в демократичних інституціях і соціальні розколи, як це яскраво демонструють ескалаційні плани на 2025 рік, спрямовані на експлуатацію внутрішніх проблем України для створення керованого хаосу через координовані інформаційні операції.

Методологія включає техніки "вогнища брехні" (firehose of falsehood), коли масований потік суперечливих версій подій перевантажує когнітивні здатності аудиторії; "рефлексивного контролю", спрямованого на маніпулювання процесом прийняття рішень через підкидання спеціально

сконструйованої інформації; "активних заходів" з використанням реальних документів у спотвореному контексті; та "інформаційного лаундрингу", коли дезінформація відмивається через ланцюги републікацій до набуття видимості легітимності, що особливо яскраво проявилось в кейсах з «біолабораторіями», "брудною бомбою" та іншими фейками, спрямованими на дискредитацію України на міжнародній арені.

Техніка "паралельної реальності"

Концепція "паралельної реальності" представляє найбільш софістикований рівень інформаційної агресії, де замість прямої брехні конструюється альтернативний всесвіт із власною внутрішньою логікою, історією, причинно-наслідковими зв'язками та моральними координатами, який існує паралельно з об'єктивною реальністю, але повністю її заперечує, створюючи когнітивний дисонанс та епістемологічну кризу у тих, хто потрапляє під його вплив.

Яскравими прикладами стали інтерв'ю Новінського та Медінського американським журналістам у 2025 році, де реальні факти про кримінальні провадження трансформувалися в наратив про "переслідування християн", а неспровокована агресія подавалася як "превентивний захист", демонструючи, як ця техніка набуває онтологічного виміру, атакуючи саму основу реальності, стабільність ідентичності та колективну свідомість, роблячи конфлікт невидимим і всепроникним у рамках концепцій когнітивної війни, де маніпуляція сприйняттям стає ключем до стратегічного домінування.

Ця техніка особливо небезпечна тим, що вона не просто спотворює факти, а створює цілісну картину світу, де агресор стає жертвою, окупація - визволенням, геноцид - захистом, а опір агресії - провокацією, формуючи у частини міжнародної аудиторії переконання, що існують "дві правди" та потребу в "балансі" між позиціями агресора та жертви.

Платформні уразливості та цифрові виклики

Сучасні цифрові платформи, створені для максимізації залучення користувачів та монетизації уваги, стали ідеальними провідниками дезінформації через алгоритми, які пріоритизують емоційно заряджений контент, сенсаційність та controверсійність над точністю та збалансованістю, створюючи "бульбашки фільтрів" та "ехо-камери", де користувачі опиняються в замкнених інформаційних просторах, що постійно підтверджують їхні упередження та радикалізують погляди. Особливу загрозу становить екосистема Telegram, яка через поєднання анонімності, відсутності модерації, алгоритмічної непрозорості та можливості масового охоплення перетворилася на головну платформу для поширення російської дезінформації в Україні, де анонімні канали з мільйонними аудиторіями формують порядок денний, поширюють паніку, координують інформаційні атаки та підривають довіру до офіційних джерел.

Технології штучного інтелекту додали нового виміру загрозам через можливості створення гіперреалістичних дипфейків політичних лідерів, масового генерування псевдожурналістського контенту, автоматизації створення та управління ботофермами, персоналізації дезінформаційних кампаній під психологічні профілі конкретних користувачів, що робить маніпуляції практично непомітними та надзвичайно ефективними, особливо в поєднанні з викраденими персональними даними та поведінковою аналітикою, яка дозволяє визначати найбільш вразливі моменти та точки впливу на кожну цільову аудиторію.

2.2. Соціально-психологічний вимір

Інформаційна втома та падіння довіри

Феномен інформаційної втоми став масовим явищем в умовах безперервного потоку тривожних новин, суперечливих повідомлень, емоційно виснажливого контенту та постійної необхідності розрізняти правду серед океану маніпуляцій, що призводить до психологічного вигорання, апатії, зниження критичного мислення та парадоксального ефекту, коли люди починають уникати новин взагалі або, навпаки, компульсивно споживати їх без аналізу, впадаючи в стан "завченої безпорадності". Це супроводжується системним падінням довіри не лише до медіа, які сприймаються

як упереджені незалежно від їхньої реальної якості, але й до державних інституцій, експертного знання, наукових даних та самої концепції об'єктивної істини.

Особливо гостро це проявляється в умовах війни, коли необхідність у безпековій секретності конфліктує з потребою у прозорості, створюючи інформаційний вакуум, який миттєво заповнюється чутками, спекуляціями та ворожою пропагандою, а кожне спростування сприймається як приховування "справжньої правди", формуючи замкнене коло недовіри, де навіть правдива інформація від офіційних джерел автоматично ставиться під сумнів, а конспірологічні теорії набувають більшої привабливості через їхню емоційну насиченість та ілюзію розкриття прихованих смислів.

Ця втома переходить у хронічний стан, де емоційне виснаження та епістемологічна невизначеність стають нормою повсякденного існування, посилюючи соціальну ізоляцію та тотальний скептицизм, що ідеально відповідає стратегічним цілям гібридної війни - створенню суспільства, нездатного до консолідованого опору через втрату спільних смислових координат.

Вразливі групи та точки розколу

Російська дезінформація систематично експлуатує соціальні розломи та вразливості різних груп українського суспільства, використовуючи таргетовані меседжі, адаптовані під специфічні страхи, образи та фрустрації кожної аудиторії, створюючи мозаїку взаємовиключних наративів, що підривають солідарність та провокують внутрішні конфлікти. Внутрішньо переміщені особи стають мішенню наративів про "тягар для громад", "конкуренцію за ресурси" та "привілеї", що поглиблює відчуження та перешкоджає інтеграції; військові та їхні родини бомбардуються меседжами про "забутих героїв", "зраду командування" та "марність жертв", підриваючи морально-психологічний стан та провокуючи радикалізацію; молодь таргетується через наративи про "втрачене покоління", "війну за чужі інтереси" та "відсутність майбутнього", стимулюючи еміграційні настрої та соціальний нігілізм.

Мовне питання залишається постійним інструментом розколу через штучне протиставлення українськомовних та російськомовних громадян, конструювання міфу про "примусову українізацію" та "дискримінацію", ігноруючи реальність, де російськомовні українці масово підтримують незалежність та воюють проти агресора; регіональні відмінності експлуатуються через відродження штучних поділів на "справжню" та "несправжню" Україну, "бандерівців" та "нормальних людей", "Захід" та "Схід", хоча реальний досвід війни продемонстрував безпрецедентну єдність усіх регіонів у протистоянні агресії; соціально-економічні проблеми використовуються для просування наративів про "корупцію", "зраду еліт" та "потребу в сильній руці", підриваючи демократичні інститути та готуючи ґрунт для авторитарних тенденцій.

2.3. Обмеження традиційних підходів

Чому фактчекінг недостатній

Фактчекінг, попри свою важливість як інструмент верифікації інформації, виявився принципово обмеженим у протидії сучасній дезінформації, яка еволюціонувала далеко за межі простої брехні про факти, використовуючи натомість маніпуляції контекстом, емоційні тригери, напівправди, селективну подачу реальних фактів у спотвореній інтерпретації та конструювання альтернативних смислових рамок, де факти можуть бути технічно правильними, але висновки - абсолютно хибними.

Фундаментальна проблема полягає в асиметрії зусиль: створення фейку займає секунди та не вимагає ресурсів, тоді як його спростування потребує годин роботи кваліфікованих експертів, доступу до джерел, написання детального розбору, який охопить набагато меншу аудиторію, ніж оригінальна брехня, та прийде надто пізно, коли шкода вже завдана, а увага громадськості переключилася на нові теми.

Психологічні дослідження демонструють ефект "продовження впливу" (continued influence effect), коли навіть після спростування люди продовжують вірити в дезінформацію, особливо якщо вона відповідає їхнім упередженням або емоційним потребам; ефект "зворотного вогню" (backfire effect), коли спроби спростування лише посилюють віру в конспірологічні теорії через сприйняття фактчекерів як частини "системи приховування правди"; та "ілюзію правди" (illusory truth effect), коли багаторазове повторення брехні, навіть у контексті її спростування, підвищує ймовірність того, що люди в неї повірять, роблячи традиційний фактчекінг не просто неефективним, але потенційно контрпродуктивним.

Проблема реактивного реагування

Реактивна модель інформаційної оборони, побудована на принципі відповіді на вже здійснені інформаційні атаки, прирікає захисників на постійне відставання в динаміці інформаційної війни, де ініціатива завжди належить агресору, який визначає порядок денний, нав'язує теми дискусії, контролює темп та інтенсивність конфронтації, змушуючи противника витратити ресурси на гасіння інформаційних пожеж замість реалізації власної стратегії. Ця модель створює замкнене коло, де кожне спростування легітимізує фейк через саму необхідність на нього реагувати, надаючи йому додаткову видимість та важливість; де захисники постійно грають на полі, правила якого встановлює агресор; де стратегічне планування підміняється тактичним реагуванням, а довгострокові цілі приносяться в жертву короткостроковим кризам.

Особливо руйнівним є ефект "стратегічного паралічу", коли безперервний потік криз унеможливорює стратегічне мислення та планування, організації працюють у режимі постійної надзвичайної ситуації, виснажуються людські та фінансові ресурси, втрачається здатність до проактивної дії, а вся система переходить у режим виживання замість розвитку, що є однією з цілей гібридної агресії - виснажити противника не стільки фізично, скільки морально та організаційно, довести його до стану, коли опір стає неможливим не через брак ресурсів, а через втрату волі та віри в перемогу.

Парадокс "більше інформації – менше довіри"

Інформаційна епоха породила парадоксальну ситуацію, коли безпрецедентний доступ до інформації не призвів до кращого розуміння реальності, а навпаки - створив епістемологічну кризу, де надлишок інформації перевантажує когнітивні здатності людей, унеможливорює розрізнення важливого та другорядного, правди та брехні, експертного знання та дилетантських думок, формуючи інформаційний хаос, у якому орієнтація стає неможливою без спрощення, а спрощення веде до спотворення. Демократизація виробництва та поширення інформації, яка мала б посилити громадянське суспільство, натомість підірвала традиційні механізми верифікації та легітимації знання, коли кожен може бути "експертом", будь-яка думка претендує на рівноцінність з науковим знанням, а емоційний резонанс стає важливішим за фактичну точність.

Цей парадокс поглиблюється алгоритмічною фільтрацією, яка, намагаючись зробити інформаційний потік керованим, створює "бульбашки фільтрів", де люди бачать лише те, що підтверджує їхні погляди; монетизацією уваги, яка робить сенсаційність та контрверсійність більш прибутковими за точність та збалансованість; кризою експертизи, коли складність сучасних проблем перевищує здатність неспеціалістів їх зрозуміти, але недовіра до експертів робить їхнє знання соціально нерелевантним; що в сукупності створює ситуацію, де збільшення кількості доступної інформації веде не до кращої інформованості, а до глибшої дезорієнтації, не до консенсусу на основі фактів, а до фрагментації на основі наративів, не до раціонального дискурсу, а до емоційної поляризації.

РОЗДІЛ III. ADVANCE TRUTH STRATEGY (ATS)

3.1. Парадигмальний зсув

Від спростування фейків до формування смислових рамок

Advance Truth Strategy представляє фундаментальний парадигмальний зсув в підходах до інформаційної оборони, де замість виснажливої та безперспективної гри в "інформаційний пінг-понг"

спростування кожного окремого фейку пропонується стратегія превентивного формування стійких смислових рамок - глибинних когнітивних структур, які визначають, як люди інтерпретують інформацію ще до того, як вона потрапляє в їхнє поле зору, створюючи своєрідний "ментальний імунітет" проти маніпуляцій. Ці смислові рамки функціонують як епістемологічні фільтри, через які проходить вся вхідна інформація, автоматично відсіюючи явно маніпулятивний контент не через раціональний аналіз кожного твердження, а через несумісність з базовими ціннісними координатами та картиною світу, що робить дезінформацію не просто неправдоподібною, але онтологічно чужорідною для свідомості реципієнта.

Формування таких рамок передбачає не реактивне заперечення ворожих наративів, а проактивне насичення інформаційного простору власними смислами, історіями, символами та метафорами, які створюють цілісну картину реальності, де українська перспектива стає не однією з можливих інтерпретацій, а природною точкою відліку для розуміння подій, перетворюючи громадян з пасивних споживачів інформації на активних співтворців смислів, здатних не лише розпізнавати маніпуляції, але й самостійно генерувати контрнативи на основі інтерналізованих цінностей та переконань.

Від боротьби з наративами до створення метанаративів

Традиційна модель протидії дезінформації, зосереджена на боротьбі з окремими ворожими наративами, виявилася стратегічно програшною, оскільки вона приречена на постійне реагування на нескінченний потік нових історій, версій та інтерпретацій, кожна з яких вимагає окремих зусиль для спростування, розпорошуючи ресурси та увагу, створюючи фрагментований інформаційний ландшафт без єдиної об'єднуючої логіки. ATS пропонує перехід на вищий рівень абстракції через створення метанаративів - великих об'єднуючих історій, які не просто заперечують окремі брехливі твердження, а пропонують альтернативну космологію, де українська боротьба постає не як локальний конфлікт за територію чи владу, а як епічне протистояння між свободою та тиранією, між майбутнім та минулим, між гідністю та рабством, що резонує з універсальними людськими цінностями та архетипами.

Метанаративи працюють на рівні глибинних психологічних структур, активуючи архетипічні образи героя, що долає випробування; спільноти, яка об'єднується перед загрозою; світла, що перемагає темряву - створюючи емоційно насичену матрицю сприйняття, в якій кожна нова подія автоматично вписується в загальну логіку боротьби добра зі злом, правди з брехнею, свободи з поневоленням, роблячи ворожі наративи не просто хибними, але естетично та морально відразливими, несумісними з базовими людськими прагненнями до справедливості, свободи та гідності.

Від гри за правилами ворога до встановлення власних правил

Найбільш руйнівним аспектом традиційної інформаційної оборони є прийняття правил гри, нав'язаних агресором - необхідність реагувати на його провокації, спростовувати його твердження, працювати в його темпі та за його порядком денним, що автоматично ставить захисника в програшну позицію того, хто завжди наздоганяє, виправдовується та грає на чужому полі. ATS кардинально змінює цю динаміку через встановлення власних правил інформаційної гри, де Україна не відповідає на ворожі наративи, а ігнорує їх, створюючи власний інформаційний всесвіт з власною логікою, темами, героями та антигероями, змушуючи противника реагувати на українські ініціативи, спростовувати українські твердження, грати за українськими правилами.

Це означає свідому відмову від дебатів на території, визначеній ворогом - замість дискусії про "нацизм в Україні" формується дискурс про російський фашизм; замість виправдань щодо "дискримінації російськомовних" створюється наратив про геноцид українців; замість реакції на звинувачення в "агресивності НАТО" просувається тема російського імперіалізму як загрози глобальній безпеці, перетворюючи інформаційну оборону з пасивного захисту на активний наступ, де кожна відповідь стає приводом для контратаки, кожне спростування - можливістю для просування власного порядку денного.

3.2. Механізми проактивної дії

Створення контрреальності

Механізм створення контрреальності виходить за межі простого спростування ворожих фейків чи пропонування альтернативних фактів - це конструювання цілісного паралельного інформаційного всесвіту, який не просто заперечує російську "паралельну реальність", але повністю її заміщує більш привабливою, логічною та емоційно резонуючою картиною світу, де кожен елемент російської пропаганди автоматично перетворюється на свою протилежність через зміну інтерпретаційної матриці. У цій контрреальності російські твердження про "захист російськомовних" трансформуються в наратив про колоніальну експлуатацію; заяви про "денацифікацію" - у викриття російського нацизму; розмови про "братські народи" - у розкриття геноцидної природи російського режиму, створюючи дзеркальне відображення, де кожна брехня працює проти того, хто її породив.

Ця контрреальність будується не на запереченні, а на переосмисленні, не на обороні, а на наступі, не на реакції, а на ініціативі, використовуючи силу ворожих наративів проти них самих через техніку "інформаційного айкідо", коли енергія атаки спрямовується на поразку атакуючого, перетворюючи кожную спробу дезінформації на можливість для розкриття справжньої природи агресора, його методів, цілей та слабкостей, роблячи його власну пропаганду найкращим свідченням проти нього самого.

Глибинні рамки сприйняття

Робота з глибинними рамками сприйняття представляє найбільш софістикований рівень інформаційного впливу, який діє не на рівні свідомих переконань чи раціональних аргументів, а на рівні базових когнітивних структур, що визначають, як людина категоризує реальність, що вважає можливим чи неможливим, природним чи протиприродним, моральним чи аморальним, ще до того, як починається будь-який свідомий аналіз. Ці рамки формуються через систематичне використання метафор, які структурують мислення (війна як "визвольна боротьба", а не "конфлікт"; Росія як "імперія зла", а не "сусідня держава"); архетипічних образів, що активують глибинні психологічні програми (Україна як Давид проти Голіафа, як фенікс, що відроджується); та емоційних якорів, які прив'язують певні почуття до певних концептів (гордість до опору, відразу до колабораціонізму).

Формування таких рамок вимагає довготривалої систематичної роботи через всі канали комунікації - від офіційних заяв до популярної культури, від освітніх програм до соціальної реклами, створюючи когнітивне середовище, де українська перспектива стає "здоровим глуздом", природною точкою відліку для оцінки будь-якої інформації, автоматичним фільтром, який відсіює маніпуляції ще до того, як вони досягнуть порогу свідомого сприйняття, перетворюючи кожного громадянина на носія імунітету проти інформаційних вірусів.

Технології випередження

Технології випередження базуються на принципі превентивної інокуляції інформаційного простору проти майбутніх атак через завчасне формування контрнативів до того, як ворог встигне запустити свої дезінформаційні кампанії, використовуючи прогностичну аналітику для визначення ймовірних векторів атак та підготовки інформаційних "вакцин" - попереджувальних меседжів, які роблять аудиторію несприйнятливою до певних типів маніпуляцій. Це включає техніку "пребанкінгу" (pre-bunking) - завчасного викриття методів маніпуляції до того, як вони будуть застосовані; "нормативного щеплення" - формування стійких норм та очікувань щодо того, яка інформація є прийнятною; та "сценарного програмування" - підготовки громадськості до різних варіантів розвитку подій через попереднє програвання можливих сценаріїв.

Випереджувальні технології також включають створення "інформаційних пасток" - навмисне формування інформаційних приводів, які провокують ворога на передбачувані дії, що дискредитують його в очах аудиторії; "каскадне програмування" - запуск ланцюгових реакцій, де кожна наступна подія підсилює попередній меседж; та "темпоральне домінування" - контроль над часовими параметрами інформаційних кампаній, коли власні меседжі завжди випереджають ворожі, задаючи рамку для їх сприйняття та інтерпретації.

3.3. Практичні інструменти ATS

Ситуаційні кімнати та системи раннього виявлення

Ситуаційні кімнати в концепції ATS мають бути собою високотехнологічними центрами інформаційного моніторингу та аналізу, які функціонують як "нервові центри" системи інформаційної оборони, інтегруючи в режимі реального часу потоки даних з усіх доступних джерел - від традиційних медіа до соціальних мереж, від експертних оцінок до алгоритмічного аналізу, створюючи цілісну картину інформаційного поля битви з візуалізацією трендів, аномалій, кореляцій та прогнозів. Ці центри мають працювати за принципом "тотальної ситуаційної обізнаності", коли кожен інформаційний сигнал аналізується не ізольовано, а в контексті загальної динаміки, виявляючи приховані зв'язки між начебто незалежними подіями, розпізнаючи координовані кампанії на ранніх стадіях, прогножуючи ескалацію та визначаючи оптимальні точки для превентивного втручання.

Системи раннього виявлення мають використовувати комбінацію людського експертного аналізу та машинного навчання для розпізнавання "слабких сигналів" - ледь помітних змін в інформаційних паттернах, які передують масштабним дезінформаційним атакам, таких як аномальна активність ботів, синхронізовані зміни риторики в різних каналах, появу нових наративних конструкцій, координовані зміни в алгоритмічній видачі, що дозволяє запускати превентивні контрзаходи до того, як ворожа кампанія набере критичної маси та стане некерованою.

РОЗДІЛ IV. ІНСТИТУЦІЙНА АРХІТЕКТУРА

4.1. Державний рівень

Роль стратегічних комунікацій

Стратегічні комунікації на державному рівні мають трансформуватися з допоміжної функції інформування громадськості в центральний елемент національної безпеки та оборонної демократії, де має бути забезпечена координація меседжів між усіма гілками влади, міністерствами та відомствами для створення єдиної симфонії смислів, що резонуватиме через усі канали державної комунікації, від офіційних заяв президента до повідомлень місцевих адміністрацій, формуючи цілісну картину державної позиції без суперечностей та дисонансів, які могли б експлуатувати вороги. Ця система повинна вийти за межі традиційного прес-службового підходу, перетворюючись на стратегічний механізм формування реальності, де кожне державне повідомлення розглядатиметься не як окрема інформаційна одиниця, а як елемент загального наративу, що будуватиме довготривалі смислові конструкції в свідомості громадян та міжнародної спільноти, створюючи стійкі патерни сприйняття України як успішної демократії, що героїчно протистоїть агресії та буде європейське майбутнє.

Має бути створено реально потужний Центр стратегічних комунікацій та інформаційної війни, який функціонуватиме як мозковий центр цієї системи, інтегруючи розвідувальну інформацію про інформаційні загрози, соціологічні дані про суспільні настрої, експертні оцінки трендів та прогнози розвитку ситуації в єдину аналітичну картину, на основі якої формуватимуться довгострокові комунікаційні стратегії та оперативні плани реагування, забезпечуючи проактивність державної комунікації, її випереджувальний характер та здатність формувати порядок денний замість реагування на нав'язані теми.

На прикладі програних росії комунікацій мобілізації та ударів по енергетичній інфраструктурі слід зробити висновки та картографію реагування. У випадку мобілізації – не потрібно чекати коли росія оприлюднить свою версію «бусифікації», кожен потенційно загрозливий випадок має комунікуватися з державних інтересів. Повідомлення про знищення ТЕС не мають звучати як апокаліптичні прогнози в період коли ще не почалися морози.

Координаційні механізми

Координаційна архітектура інформаційної оборони на державному рівні має бути вибудована як багаторівнева мережа горизонтальних та вертикальних зв'язків, де Рада національної безпеки і оборони повинна виступати стратегічним координатором, визначаючи загальні пріоритети та червоні лінії; Центр протидії дезінформації, після оновлення, має забезпечувати оперативну координацію між

силовими структурами та цивільними відомствами; міжвідомчі робочі групи повинні синхронізувати зусилля в конкретних тематичних напрямках; а регіональні координаційні центри, які слід створити, адаптуватимуть національні стратегії до локальних контекстів, формуючи безшовну систему, де інформація та рішення циркулюватимуть без затримок та спотворень. Ця система має працювати за принципом "розподіленої відповідальності з централізованою координацією", коли кожен актор матиме чітко визначену зону компетенції та автономію в межах своїх повноважень, але всі дії синхронізуватимуться через єдиний координаційний центр, що забезпечить синергію зусиль та уникнення дублювання чи протиріч.

Особливо важливо розробити механізми швидкої ескалації та кризового реагування, коли виявлення серйозної інформаційної загрози автоматично запускатиме протоколи залучення всіх релевантних акторів, від спецслужб до громадських організацій, створюючи тимчасові оперативні штаби з надзвичайними повноваженнями для координації протидії, що дозволить концентрувати ресурси та увагу на критичних точках інформаційного протистояння. Це особливо актуально поєднувати з реагуванням на кінетичні загрози, уникаючи звинувачень в штучній пропаганді.

Законодавче забезпечення

Законодавча база інформаційної оборони має бути сформована як складна система правових норм, що балансуватимуть між необхідністю захисту національного інформаційного простору та збереженням фундаментальних свобод, створюючи правові механізми протидії дезінформації без сповзання в цензуру, забезпечуючи прозорість медіавласності без порушення права на приватність, встановлюючи відповідальність за свідоме поширення шкідливого контенту без криміналізації помилок та непорозумінь. Ключовим принципом законодавчого регулювання має стати "презумпція свободи з точковими обмеженнями", коли будь-які рестрикції застосовуватимуться лише в чітко визначених випадках реальної та безпосередньої загрози національній безпеці, з обов'язковим судовим контролем та можливістю оскарження, створюючи систему стримувань та противаг, що унеможливить зловживання.

Критично важливо забезпечити гармонізацію національного законодавства з європейськими стандартами, що забезпечить інтеграцію України в європейський простір цифрової безпеки та створить правові підстави для транскордонної співпраці в протидії дезінформації, включаючи механізми швидкого видалення шкідливого контенту, накладення санкцій на платформи за недотримання стандартів та координації зусиль з європейськими партнерами.

4.2. Громадянське суспільство

Мережі фактчекінгу та медіаграмотності

Громадянські мережі фактчекінгу мають еволюціонувати від розрізнених ініціатив ентузіастів до потужної розгалуженої інфраструктури верифікації інформації, що охоплюватиме всі регіони країни та основні тематичні напрямки, об'єднуючи професійних журналістів, експертів, науковців та волонтерів у спільну екосистему, де кожен учасник вноситиме свою унікальну експертизу та ресурси, створюючи колективний розум, здатний швидко розпізнавати та нейтралізувати дезінформаційні атаки. Ці мережі повинні функціонувати за принципом "розподіленої верифікації", коли первинна перевірка здійснюватиметься локальними волонтерами, поглиблений аналіз - спеціалізованими експертами, а фінальна верифікація та публікація - професійними фактчекінговими організаціями, забезпечуючи багаторівневий контроль якості та швидкість реагування.

Програми медіаграмотності необхідно трансформувати з факультативних освітніх ініціатив у системну національну програму формування критичного мислення, що охоплюватиме всі вікові групи та соціальні верстви через формальну освіту в школах та університетах, неформальну освіту в бібліотеках та громадських центрах, корпоративні тренінги для працівників, спеціалізовані курси для вразливих груп, створюючи суцільне покриття суспільства навичками розпізнавання маніпуляцій, верифікації інформації та усвідомленого медіаспоживання, перетворюючи кожного громадянина на активного учасника інформаційної оборони.

Центри життєстійкості в громадах

Центри життєстійкості мають бути створені як інноваційна форма громадської самоорганізації для протидії комплексним викликам війни, об'єднуючи в одному просторі функції психологічної підтримки, інформаційної безпеки, соціальної інтеграції та громадського діалогу, формуючи безпечні гавані в морі невизначеності та стресу, де люди зможуть отримати допомогу, підтримку, достовірну інформацію та відчуття спільноти. Ці центри повинні функціонувати як мультифункціональні хаби, що надаватимуть психологічні консультації для подолання травм війни; проводитимуть тренінги з медіаграмотності та цифрової безпеки; організовуватимуть діалогові майданчики між різними групами громади; координуватимуть волонтерську допомогу та взаємопідтримку; створюватимуть простір для культурних заходів та збереження ідентичності, формуючи навколо себе стійкі спільноти, здатні протистояти викликам.

Особливу увагу слід приділити ролі центрів в інтеграції внутрішньо переміщених осіб, ветеранів, родин військовослужбовців та інших вразливих груп, створюючи містки між різними сегментами громади через спільні проєкти, взаємодопомогу та діалог, руйнуючи стереотипи та упередження, будуючи горизонтальні зв'язки довіри та солідарності, що зробить громади стійкішими до розколів та маніпуляцій, перетворюючи потенційні точки напруги на джерела взаємного збагачення та зміцнення.

Роль церков та релігійних організацій

Церкви та релігійні організації мають стати важливими акторами інформаційної оборони, використовуючи свій особливий моральний авторитет, довіру громад та розгалужені мережі для донесення важливих меседжів до аудиторій, недосяжних для офіційних каналів, особливо серед старшого покоління, сільських громад та консервативних верств населення. Релігійні лідери повинні виступити як "амбасадори правди", використовуючи проповіді, пастирські бесіди та релігійні медіа для протидії дезінформації, спростування маніпулятивних наративів про "релігійні переслідування", формування стійких моральних орієнтирів в умовах інформаційного хаосу, надання духовної підтримки в подоланні травм та збереженні надії.

Необхідно розвивати міжконфесійний діалог та співпрацю різних релігійних організацій для створення потужного фронту протидії спробам розколу суспільства за релігійною ознакою, демонструючи єдність різних конфесій у захисті України, спільні цінності та взаємоповагу, що руйнуватиме російські наративи про "релігійну війну" та підкреслюватиме справжню природу конфлікту як боротьби за свободу та гідність, де віруючі всіх конфесій об'єднуються проти агресора, що намагається використати релігію як інструмент поневолення.

4.3. Медіа-екосистема

Суспільне мовлення як якір довіри

Суспільне мовлення має бути трансформоване з традиційної телерадіокомпанії в мультиплатформенний центр довіри, що поєднуватиме класичне телебачення та радіо з потужною цифровою присутністю, стрімінговими сервісами, подкастами та соціальними медіа, створюючи всеохоплюючу мережу достовірної інформації, доступної для всіх верств населення через їхні улюблені канали споживання контенту. Незалежність від політичного та комерційного тиску має бути забезпечена через систему громадського управління та фінансування, що дозволить суспільному мовнику виконувати роль "золотого стандарту" журналістики, встановлюючи еталони якості, об'єктивності та етики для всієї медіаіндустрії, створюючи острів довіри в морі інформаційного шуму.

Особливу увагу слід приділити підготовці суспільного мовлення до роботи в кризових ситуаціях, коли воно має стати головним джерелом офіційної інформації, координуючи інформаційні потоки між владою та громадянами, забезпечуючи безперервність комунікації навіть в умовах відключень електроенергії чи інтернету через резервні канали та системи оповіщення, підтримуючи суспільний спокій та організованість через надання чітких інструкцій, спростування панічних чуток та формування відчуття контрольованості ситуації.

Локальні медіа та регіональна стійкість

Локальні медіа мають отримати системну підтримку для виконання критичної ролі у формуванні інформаційної стійкості на рівні громад, використовуючи свою близькість до людей та високий рівень довіри через особисте знайомство з журналістами, розуміння локального контексту та здатність швидко реагувати на місцеві проблеми та виклики. Необхідно створити програми підтримки локальних медіа через гранти, навчальні програми, технічну допомогу та захист від тиску, формуючи густу мережу інформаційних вузлів, що покриватимуть всю територію країни, забезпечуючи доступ до якісної журналістики навіть у найвіддаленіших куточках, де національні медіа можуть бути недоступними або нерелевантними.

Слід створити регіональні медіахаби як центри підтримки локальної журналістики, що надаватимуть спільні ресурси та гранти для розслідувань, юридичну підтримку, технічну інфраструктуру та навчання, створюючи економію масштабу для малих редакцій та підвищуючи якість локального контенту, формуючи мережі співпраці між локальними медіа для обміну контентом, спільних проєктів та взаємопідтримки, що зробить локальну журналістику більш стійкою економічно та професійно.

Етика та саморегуляція

Система медійної етики та саморегуляції має еволюціонувати від формальних кодексів та декларацій до живої культури професійної відповідальності, де журналістська спільнота самостійно встановлюватиме та підтримуватиме високі стандарти через механізми колегіального контролю, професійної солідарності та репутаційних санкцій, створюючи середовище, де порушення етики стане не просто формальним проступком, але соціально неприйнятним вчинком, що веде до втрати професійної репутації та можливостей. Комісія з журналістської етики має бути посилена для функціонування як незалежний арбітр, розглядаючи скарги на порушення стандартів, виносячи публічні рішення та рекомендації, формуючи прецедентну практику етичних норм, проводячи освітні заходи та консультації, створюючи культуру постійного вдосконалення професійних стандартів.

Роль держави, в контексті вищенаведеного в цьому розділі, має бути партнерська та регулятивна, що встановлює єдині правила для всіх. Також державні органи мають надавати всю повноту інформації в межах їх компетенцій, не лишаючи простору для спекуляцій. В жодному разі побудова стратегічних комунікацій не може ставати містком для тотальної цензури. Цей баланс – ключовий принцип оборонної демократії в інформаційній сфері.

РОЗДІЛ V. ОПЕРАЦІЙНА МОДЕЛЬ «INFOLIGHT.UA – 2026»

Представлена операційна модель є проєктним баченням функціонування Дослідницько-аналітичної групи INFOLIGHT.UA на 2026 рік за умови наявності належного фінансування та підтримки партнерів. Команда проєкту готова стати стратегічним партнером держави та взяти на себе виконання частини функцій інформаційної оборони, використовуючи накопичену експертизу, напрацьовані методології та мережу контактів для посилення національної стійкості в інформаційному просторі.

Компоненти системи

Центр моніторингу та аналітики

Центр моніторингу та аналітики має стати операційним ядром проєкту INFOLIGHT.UA – 2026, функціонуючи як високотехнологічна платформа безперервного спостереження за інформаційним простором, що інтегруватиме потоки даних з традиційних медіа, соціальних мереж, месенджерів, форумів та інших цифрових платформ у єдину аналітичну систему реального часу. Система має використовувати комбінацію алгоритмічного моніторингу через штучний інтелект та машинне навчання для первинної обробки масивів даних з обов'язковою експертною валідацією людиною для глибинного аналізу контексту, виявлення прихованих смислів та розпізнавання складних маніпулятивних технік, що виходять за межі можливостей автоматизованих систем.

Ключовим продуктом Центру мають стати щоденні аналітичні брифи для ключових стейкхолдерів, щотижневі звіти про наративні тренди для медіа та громадських організацій, оперативні сповіщення

про виявлені дезінформаційні кампанії для органів влади, а також публічні дашборди з візуалізацією інформаційних потоків для широкого загалу, що забезпечить прозорість роботи системи та підвищить обізнаність суспільства про інформаційні загрози. Особливу увагу слід приділити розробці системи "карток фейків" - стандартизованих описів дезінформаційних кампаній з детальним розбором методів, цільових аудиторій, каналів поширення та рекомендацій щодо протидії, що створить базу знань для всіх учасників інформаційної оборони.

Лабораторія швидкої відповіді

Лабораторія швидкої відповіді має бути організована як креативний хаб з виробництва контрконтенту, що працюватиме в режимі 24/7 з можливістю мобілізації додаткових ресурсів у кризових ситуаціях, об'єднуючи професійних контент-мейкерів, графічних дизайнерів, відеомонтажерів, копірайтерів, сценаристів та психологів у міждисциплінарні команди, здатні створювати високоякісний мультимедійний контент під конкретні комунікаційні завдання. Лабораторія має розробити та постійно оновлювати бібліотеку шаблонів для різних форматів контенту - від текстових спростувань до відеороликів, від інфографіки до інтерактивних презентацій, що дозволить скоротити час виробництва з годин до хвилин у критичних ситуаціях.

Особливо важливо забезпечити здатність Лабораторії до "контекстуальної адаптації" - створення версій одного меседжу, оптимізованих під психологічні профілі різних цільових аудиторій: раціональні аргументи для інтелектуальної еліти, емоційні історії для широкого загалу, візуальні меми для молоді, авторитетні заяви для старшого покоління, забезпечуючи максимальну ефективність комунікації через врахування особливостей сприйняття кожної групи. Лабораторія також має розробити протоколи "випереджувального контенту" - підготовку матеріалів для ймовірних дезінформаційних атак на основі прогностичної аналітики, що дозволить миттєво реагувати на передбачувані провокації.

Мережа локальних інформаційних хабів

Мережа локальних інформаційних хабів має бути розгорнута як система регіональних партнерств з місцевими медіа, громадськими організаціями, освітніми закладами та активістами, що створить розподілену інфраструктуру верифікації та поширення достовірної інформації на місцевому рівні. Кожен хаб функціонуватиме як вузол двостороннього обміну: збираючи інформацію про локальні дезінформаційні кампанії та передаючи її до центрального моніторингу, а також адаптуючи національні контрнаративи до місцевого контексту та поширюючи їх через довірені локальні канали.

Хаби мають працювати за принципом мережевої організації без жорсткої ієрархії, об'єднуючи місцевих журналістів, блогерів, громадських діячів, освітян та волонтерів у гнучкі коаліції, здатні швидко мобілізуватися для протидії локальним інформаційним загрозам, використовуючи знання місцевої специфіки, довіру громади та неформальні канали комунікації, недоступні для централізованих структур.

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

Ключові висновки дослідження

Проведене дослідження концепції оборонної демократії в інформаційній сфері, розробленої Українським безпековим клубом у 2025 році, дозволяє сформулювати фундаментальний висновок про необхідність парадигмального зсуву в підходах до інформаційної оборони від реактивного спростування дезінформації до проактивного формування стійких смислових рамок, від боротьби з окремими фейками до створення цілісних метанаративів, від гри за правилами агресора до встановлення власних правил інформаційного протистояння. Україна, перебуваючи в епіцентрі найбільш інтенсивної інформаційної війни сучасності, накопичила унікальний досвід протидії системній дезінформації в умовах онтологічної атаки на саму природу реальності, ідентичності та колективного буття, що робить її природною лабораторією для розробки та тестування інноваційних підходів до захисту демократії в цифрову епоху.

Аналіз загроз та викликів виявив безпрецедентну складність сучасної російської дезінформаційної машини, яка еволюціонувала від традиційної пропаганди до комплексної системи когнітивної війни, використовуючи весь спектр технологій від ботоферм до глибоких фейків, від маніпуляцій алгоритмами до конструювання паралельних реальностей, що вимагає відповідної складності та софістикованості систем протидії. Соціально-психологічний вимір інформаційних загроз демонструє глибоку трансформацію суспільної свідомості під впливом інформаційної втоми, падіння довіри до всіх джерел інформації та культурно-мовної дезорієнтації, що створює сприятливе середовище для маніпуляцій та потребує комплексних зусиль з відновлення епістемологічної стійкості суспільства.

Advance Truth Strategy (ATS) як інноваційний підхід до інформаційної оборони пропонує перехід від оборонної до наступальної позиції через створення власної контрреальності, формування глибинних рамок сприйняття та використання технологій випередження, що дозволяє не просто реагувати на ворожі атаки, але формувати інформаційне поле таким чином, щоб дезінформація ставала неефективною ще до її появи. Практичні інструменти ATS - ситуаційні кімнати, лабораторії швидкої відповіді, мережі довіри - демонструють можливість побудови розподіленої, але скоординованої системи інформаційної оборони, що поєднує технологічну софістикованість з людським виміром довіри та солідарності.

Інституційна архітектура оборонної демократії має базуватися на принципі багаторівневої взаємодії, де державний рівень забезпечує стратегічну координацію та правові рамки, громадянське суспільство формує мережі довіри та медіаграмотності, медіа-екосистема створює якісний контент та підтримує етичні стандарти, а міжнародне партнерство забезпечує обмін досвідом та координацію зусиль, створюючи синергетичний ефект, коли сума частин перевищує їхню просту суму. Критично важливим є збереження балансу між необхідністю захисту інформаційного простору та фундаментальними свободами, уникнення спокуси авторитарних рішень та збереження демократичної природи системи навіть в умовах екзистенційної загрози.

Стратегічні рекомендації

Для державних органів:

Необхідно терміново створити потужний Центр стратегічних комунікацій та інформаційної війни з надзвичайними повноваженнями та достатнім фінансуванням, що об'єднає розвідувальні, аналітичні, комунікаційні та операційні функції під єдиним керівництвом, забезпечуючи швидкість прийняття рішень та координацію дій усіх державних акторів в інформаційному просторі. Слід розробити та впровадити національну стратегію інформаційної стійкості на основі концепції оборонної демократії, що визначить чіткі цілі, пріоритети, ресурси та механізми координації для всіх учасників системи інформаційної оборони, від центральних органів влади до локальних громад.

Критично важливо забезпечити гармонізацію законодавства з європейськими стандартами регулювання цифрового простору, створюючи правові механізми швидкого реагування на дезінформаційні кампанії без порушення фундаментальних свобод, встановлюючи чіткі процедури, судовий контроль та механізми оскарження для уникнення зловживань. Держава має виступити не монополістом інформаційної оборони, а координатором та фасилітатором зусиль усього суспільства, створюючи умови, ресурси та правові рамки для ефективної діяльності громадських організацій, медіа та приватного сектору в сфері протидії дезінформації.

Для громадянського суспільства:

Громадські організації мають об'єднати зусилля в створенні національної мережі фактчекінгу та медіаграмотності, що охопить всі регіони та соціальні групи, використовуючи синергію експертизи, ресурсів та каналів комунікації різних організацій для максимального впливу. Необхідно розвивати горизонтальні мережі довіри на рівні громад, створюючи стійкі соціальні зв'язки, що можуть протистояти спробам розколу та маніпуляцій, перетворюючи потенційні точки напруги на джерела солідарності та взаємопідтримки.

Особливу увагу слід приділити роботі з вразливими групами населення - ветеранами, внутрішньо переміщеними особами, молоддю, старшим поколінням - розробляючи спеціалізовані програми

підтримки, що враховують їхні специфічні потреби, травми та інформаційні вразливості, створюючи безпечні простори для діалогу та взаємодопомоги. Громадянське суспільство має виступити мостом між державою та громадянами, перекладаючи офіційні меседжі на зрозумілу мову, адаптуючи їх до локальних контекстів та забезпечуючи зворотний зв'язок про реальні настрої та проблеми на місцях.

Для медіа-індустрії:

Медіа мають усвідомити свою особливу відповідальність в умовах інформаційної війни та добровільно прийняти підвищені стандарти верифікації інформації, прозорості власності та етичної поведінки, розуміючи, що довіра аудиторії є їхнім головним активом, який легко втратити та важко відновити. Необхідно розвивати культуру професійної солідарності та взаємодопомоги, коли медіа не конкурують в поширенні сенсацій та фейків, а співпрацюють у верифікації інформації, обміні даними та спільному протистоянні дезінформаційним кампаніям.

Локальні медіа потребують особливої підтримки та розвитку як критично важливі елементи інформаційної екосистеми, найближчі до громад та здатні забезпечити достовірну інформацію на місцевому рівні, протидіючи локальним маніпуляціям та чуткам, що часто стають джерелом паніки та дестабілізації. Медіа-індустрія має інвестувати в навчання журналістів навичкам роботи в умовах інформаційної війни, включаючи цифрову безпеку, верифікацію контенту, розпізнавання маніпуляцій та психологічну стійкість, створюючи нове покоління медіапрофесіоналів, здатних працювати в екстремальних умовах.

Розділ V затверджено. Переходимо до Висновків та рекомендацій.

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

Ключові висновки дослідження

Проведене дослідження концепції оборонної демократії в інформаційній сфері, розробленої Українським безпековим клубом у 2025 році, дозволяє сформулювати фундаментальний висновок про необхідність парадигмального зсуву в підходах до інформаційної оборони від реактивного спростування дезінформації до проактивного формування стійких смислових рамок, від боротьби з окремими фейками до створення цілісних метанаративів, від гри за правилами агресора до встановлення власних правил інформаційного протистояння. Україна, перебуваючи в епіцентрі найбільш інтенсивної інформаційної війни сучасності, накопичила унікальний досвід протидії системній дезінформації в умовах онтологічної атаки на саму природу реальності, ідентичності та колективного буття, що робить її природною лабораторією для розробки та тестування інноваційних підходів до захисту демократії в цифрову епоху.

Аналіз загроз та викликів виявив безпрецедентну складність сучасної російської дезінформаційної машини, яка еволюціонувала від традиційної пропаганди до комплексної системи когнітивної війни, використовуючи весь спектр технологій від ботоферм до глибоких фейків, від маніпуляцій алгоритмами до конструювання паралельних реальностей, що вимагає відповідної складності та софістикованості систем протидії. Соціально-психологічний вимір інформаційних загроз демонструє глибоку трансформацію суспільної свідомості під впливом інформаційної втоми, падіння довіри до всіх джерел інформації та культурно-мовної дезорієнтації, що створює сприятливе середовище для маніпуляцій та потребує комплексних зусиль з відновлення епістемологічної стійкості суспільства.

Advance Truth Strategy (ATS) як інноваційний підхід до інформаційної оборони пропонує перехід від оборонної до наступальної позиції через створення власної контрреальності, формування глибинних рамок сприйняття та використання технологій випередження, що дозволяє не просто реагувати на ворожі атаки, але формувати інформаційне поле таким чином, щоб дезінформація ставала неефективною ще до її появи. Практичні інструменти ATS - ситуаційні кімнати, лабораторії швидкої відповіді, мережі довіри - демонструють можливість побудови розподіленої, але скоординованої системи інформаційної оборони, що поєднує технологічну софістикованість з людським виміром довіри та солідарності.

Інституційна архітектура оборонної демократії має базуватися на принципі багаторівневої взаємодії, де державний рівень забезпечує стратегічну координацію та правові рамки, громадянське суспільство формує мережі довіри та медіаграмотності, медіа-екосистема створює якісний контент та підтримує етичні стандарти, а міжнародне партнерство забезпечує обмін досвідом та координацію зусиль, створюючи синергетичний ефект, коли сума частин перевищує їхню просту суму. Критично важливим є збереження балансу між необхідністю захисту інформаційного простору та фундаментальними свободами, уникнення спокуси авторитарних рішень та збереження демократичної природи системи навіть в умовах екзистенційної загрози.

Стратегічні рекомендації

Для державних органів:

Необхідно терміново створити потужний Центр стратегічних комунікацій та інформаційної війни з надзвичайними повноваженнями та достатнім фінансуванням, що об'єднає розвідувальні, аналітичні, комунікаційні та операційні функції під єдиним керівництвом, забезпечуючи швидкість прийняття рішень та координацію дій усіх державних акторів в інформаційному просторі. Слід розробити та впровадити національну стратегію інформаційної стійкості на основі концепції оборонної демократії, що визначить чіткі цілі, пріоритети, ресурси та механізми координації для всіх учасників системи інформаційної оборони, від центральних органів влади до локальних громад.

Критично важливо забезпечити гармонізацію законодавства з європейськими стандартами регулювання цифрового простору, створюючи правові механізми швидкого реагування на дезінформаційні кампанії без порушення фундаментальних свобод, встановлюючи чіткі процедури, судовий контроль та механізми оскарження для уникнення зловживань. Держава має виступити не монополістом інформаційної оборони, а координатором та фасилітатором зусиль усього суспільства, створюючи умови, ресурси та правові рамки для ефективної діяльності громадських організацій, медіа та приватного сектору в сфері протидії дезінформації.

Для громадянського суспільства:

Громадські організації мають об'єднати зусилля в створенні національної мережі фактчекінгу та медіаграмотності, що охопить всі регіони та соціальні групи, використовуючи синергію експертизи, ресурсів та каналів комунікації різних організацій для максимального впливу. Необхідно розвивати горизонтальні мережі довіри на рівні громад, створюючи стійкі соціальні зв'язки, що можуть протистояти спробам розколу та маніпуляцій, перетворюючи потенційні точки напруги на джерела солідарності та взаємопідтримки.

Особливу увагу слід приділити роботі з вразливими групами населення - ветеранами, внутрішньо переміщеними особами, молоддю, старшим поколінням - розробляючи спеціалізовані програми підтримки, що враховують їхні специфічні потреби, травми та інформаційні вразливості, створюючи безпечні простори для діалогу та взаємодопомоги. Громадянське суспільство має виступити мостом між державою та громадянами, перекладаючи офіційні меседжі на зрозумілу мову, адаптуючи їх до локальних контекстів та забезпечуючи зворотний зв'язок про реальні настрої та проблеми на місцях.

Для медіа-індустрії:

Медіа мають усвідомити свою особливу відповідальність в умовах інформаційної війни та добровільно прийняти підвищені стандарти верифікації інформації, прозорості власності та етичної поведінки, розуміючи, що довіра аудиторії є їхнім головним активом, який легко втратити та важко відновити. Необхідно розвивати культуру професійної солідарності та взаємопідтримки, коли медіа не конкурують в поширенні сенсацій та фейків, а співпрацюють у верифікації інформації, обміні даними та спільному протистоянні дезінформаційним кампаніям.

Локальні медіа потребують особливої підтримки та розвитку як критично важливі елементи інформаційної екосистеми, найближчі до громад та здатні забезпечити достовірну інформацію на місцевому рівні, протидіючи локальним маніпуляціям та чуткам, що часто стають джерелом паніки та дестабілізації. Медіа-індустрія має інвестувати в навчання журналістів навичкам роботи в умовах

інформаційної війни, включаючи цифрову безпеку, верифікацію контенту, розпізнавання маніпуляцій та психологічну стійкість, створюючи нове покоління медіапрофесіоналів, здатних працювати в екстремальних умовах.

Для міжнародних партнерів:

Міжнародні партнери мають визнати Україну як передову лінію захисту демократичного світу від авторитарних інформаційних атак, надаючи не лише гуманітарну та військову допомогу, але й підтримку в розбудові систем інформаційної стійкості, розуміючи, що інвестиції в українську інформаційну оборону є інвестиціями у власну безпеку. Необхідно забезпечити повноцінну інтеграцію України в європейські та трансатлантичні структури інформаційної безпеки, надаючи доступ до передових технологій, методологій та розвідувальних даних, водночас використовуючи унікальний український досвід для посилення колективної стійкості.

Глобальні цифрові платформи мають визнати свою особливу відповідальність за інформаційну безпеку України, надаючи пріоритетну підтримку в модерації контенту, видаленні дезінформації та протидії координованим кампаніям, розуміючи, що Україна є полігоном, де тестуються методи маніпуляцій, які згодом будуть використані проти інших демократій. Міжнародна спільнота має підтримати створення української школи інформаційної резиліентності як центру експертизи та навчання для всього демократичного світу, визнаючи унікальну цінність українського досвіду виживання та перемоги в найінтенсивнішій інформаційній війні сучасності.

* * *

Оборонна демократія в інформаційній сфері не є тимчасовим заходом воєнного часу, а фундаментальною трансформацією підходів до захисту демократичних цінностей в епоху, коли інформація стала головною зброєю, а свідомість - головним полем битви. Україна, сплачуючи надвисоку ціну кров'ю та стражданнями, створює модель інформаційної стійкості, що може стати взірцем для всього демократичного світу, демонструючи, що навіть в умовах тотальної агресії можна не лише вижити, але й зберегти свободу, гідність та демократичну природу суспільства.

Успіх цієї моделі залежить від здатності всіх учасників - держави, громадянського суспільства, медіа, міжнародних партнерів - діяти узгоджено, синергетично та з усвідомленням спільної відповідальності за майбутнє не лише України, але й глобальної демократії, яка стоїть перед екзистенційним викликом авторитарного реваншу, озброєного найновішими технологіями маніпуляції свідомістю. Проєкт INFOLIGHT.UA – 2026 готовий стати частиною цієї колективної відповіді, пропонуючи свою експертизу, досвід та відданість справі захисту правди, свободи та людської гідності в інформаційному просторі, розуміючи, що від успіху цієї боротьби залежить не лише доля України, але й майбутнє вільного світу.