Information security and countering disinformation in complex crisis environments

Elvin Krupa*

Received: 2023-09-03
Accepted: 2023-10-02
DOI: http://dx.doi.org/10.5281/zenodo.18056832

Abstract. When reality cracks at the seams and the flow of information turns into a destructive tsunami... what is a person left with? Doubt. Panic. And a complete loss of direction. The author of this article argues that this is precisely the main goal of modern disinformation — not to convince, but to break the ability to think. It's a weapon that targets not bodies, but consciousness, destroying trust and turning society into a disoriented crowd.

Old methods of defense, like censorship, look naive in this new world. It's like trying to stop a flood by building a dam out of sand. That's why this work proposes a radically different approach. The author presents their own concept — a comprehensive, three-tiered architecture for information defense. This isn't just a collection of disparate measures. It's an attempt to create a holistic, resilient mechanism.

How does it work? First — technology. The analytical level, which uses AI for early threat detection, serves as our "eyes and ears." Then — communication. Creating unified coordination centers that speak with one, honest voice is our "nervous system." And finally, the deepest level — the cognitive one. This is about training the public in media literacy, forming a "collective immunity" to manipulation. This is our "psychological shield."

The underlying idea is to create "information sterility." This isn't about a vacuum. It's more about creating an "immune system" for society. An ecosystem where truthful, verified information spreads quickly and earns trust, while fakes and manipulations, on the contrary, get bogged down, failing to go viral. This changes the very paradigm of the fight: not chasing lies, but getting ahead of them.

Ultimately, the proposed model is not just a set of defensive measures. It's a philosophy of proactive resilience. It proves that in the modern world, information security is not the job of separate agencies. It's a collective effort. An effort of technologists, communicators, educators, and every conscious citizen.

Keywords: disinformation, information security, crisis situations, cyber threats, societal resilience, media literacy.

* Co-Chair, Committee on Civil Security and Cooperation,
International Association (UDASI)
Expert Consultant on Civil Security and on Coordination Between Local Governments, Public Safety Bodies, and Humanitarian Response Structures
Kyiv, Ukraine

Вступ

Постановка проблеми в загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Саме поняття безпеки змінилося. Невпізнанно. У XXI столітті поле битви... воно змістилося. У цифровий простір. У свідомість громадян. У стрічки новин та соціальні мережі. Інформаційні атаки... вони стали ефективнішими за фізичні удари. Вони здатні дестабілізувати цілі держави. Викликати панічні настрої. Порушити роботу систем управління. І, що найгірше, зруйнувати довіру. Довіру між громадянами та державою.

Це нова реальність. І до неї старі підходи просто стають непридатними.

Автор стверджує, що досвід країн, які опинилися в епіцентрі таких інтенсивних інформаційних протистоянь, є безцінним. Він став, по суті, живою лабораторією. Лабораторією, де в режимі реального часу довелося шукати відповіді на нові, безпрецедентні виклики. Саме цей досвід... він дозволив виробити унікальні підходи. Підходи, які можуть і повинні бути використані міжнародним співтовариством. Для зміцнення стійкості до дезінформації. І для забезпечення глобальної громадянської безпеки в нову, тривожну епоху.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спирається автор, виділення невирішених раніше частин загальної проблеми, котрим присвячується означена стаття.

Звісно, автор цієї статті не перший, хто про це говорить. Проблема не нова. Роботи таких дослідників, як П. Сінґер та Е. Брукінг [1], детально аналізують "озброєння" соціальних медіа. Класичні праці з психології мас [2] пояснюють, чому люди так легко піддаються паніці. Це важливий фундамент. Але... будемо відверті. Більшість цих робіт фокусується на діагностиці проблеми. Вони чудово пояснюють, "як це працює". Але майже ніколи — "що з цим робити" на системному, операційному рівні.

З іншого боку, є величезний пласт досліджень, присвячених технологіям. Використанню AI для виявлення фейків, як це описано в фундаментальних працях [3], що водночас узгоджується з критикою непрозорих алгоритмічних систем, викладеною, зокрема, у праці К. О'Ніл [4]. Розробці систем кіберзахисту та протидії інформаційним операціям [5]. І ось тут є проблема. Всі ці дослідження, як правило, існують у своїх вузьких "колодязях". Фахівці з кібербезпеки говорять з фахівцями з кібербезпеки. Експерти з AI — з експертами з AI.

А що залишається невирішеним? Не вирішеною залишається проблема створення єдиної, інтегрованої системи. Архітектури. Моделі, яка б об'єднала технологічні рішення, комунікаційні стратегії та освітні програми... в цілісну, працюючу операційну доктрину. Не існує універсального фреймворку. Такого, що дозволив би різним відомствам, громадським організаціям та IT-компаніям діяти синхронно. Саме цю прогалину. Цей розрив між окремими інструментами та єдиною стратегією. І покликана заповнити дана стаття.

Мета статті (постановка завдання)

Ця стаття не шукає відповіді. Вона їх дає. Автор виходить з твердої переконаності, що для боротьби з дезінформацією більше не достатньо розрізнених інструментів чи теоретичних роздумів. Потрібна цілісна, працююча архітектура. Тому головною метою цієї роботи є представлення та обґрунтування саме такої архітектури — практичної, операційної моделі інформаційного захисту.

Це, по суті, спроба покласти на стіл готове креслення. Креслення, за яким можна будувати. Автор прагне показати, як саме можна з'єднати технологічні, комунікаційні та соціальні елементи в єдиний, стійкий механізм. Механізм,

здатний не просто реагувати на загрози, а й діяти на випередження.

Для досягнення цієї мети, в наступних розділах автор детально розбере цю архітектуру на її ключові складові. Буде продемонстровано, як саме працює кожен з трьох її рівнів — аналітичний, комунікаційний та когнітивний. І як, взаємодіючи, вони створюють ефект синергії, перетворюючись на щось більше, ніж просто сума їхніх частин.

Таким чином, кінцева мета — не просто описати концепцію. А довести її життєздатність. І запропонувати її як робочу модель для побудови нового, більш ефективного інформаційного щита. Щита, здатного захистити суспільство в нову, турбулентну епоху інформаційних протистоянь.

Результати

Природа дезінформації: зброя, що цілить у свідомість

Щоб боротися з ворогом... треба зрозуміти його природу. І автор стверджує, що дезінформація — це не просто брехня. Ні. Це набагато складніша річ. Це цілеспрямована система впливу. Система, що поєднує маніпуляції, викривлення контексту та, що найстрашніше, створення альтернативної реальності, про що детально пише у своїх роботах П. Померанцев [6].

Її мета? Не переконати. А посіяти сумнів. Змусити людину втратити здатність відрізняти правду від вигадки. Занурити її у стан, який автор називає "когнітивним шумом". Цей стан, коли людина перевантажена суперечливими сигналами, ідеально експлуатує когнітивні упередження, описані Д. Канеманом [7]. І втрачає здатність до раціонального аналізу.

У кризових ситуаціях дезінформація використовується як високоточна зброя. Вона б'є по найвразливіших точках. Її цілі? Підрив довіри. Деморалізація. Руйнування соціальної солідарності. І створення керованого хаосу.

Трирівнева архітектура захисту: відповідь на виклик

Як протидіяти такій загрозі? Автор пропонує не просто набір заходів. А комплексну, трирівневу архітектуру захисту.

Перший рівень — аналітичний. Це технологічний щит. Його завдання — бачити бурю ще на горизонті. Для цього автор пропонує впровадження систем AI. Машинного навчання. І створення "інформаційних барометрів" — систем, що сигналізують про початок цілеспрямованих кампаній.

Другий — комунікаційний. Це про синергію. Ідея автора проста: зруйнувати відомчі "вежі зі слонової кістки". Замість того, щоб кожен діяв окремо... створюються єдині координаційні центри. Центри, що об'єднують державні структури, медіа, громадські організації. Їхнє завдання — виробити єдину, чесну риторику і створити довірений канал комунікації, що узгоджується з принципами проактивної комунікації, рекомендованими, зокрема, Центром стратегічних комунікацій НАТО [8].

І третій рівень... когнітивний. І ось тут, на думку автора, і криється найголовніше. Це про психологічну стійкість. Про "імунітет" суспільства. Можна збудувати найпотужніші фільтри. Але якщо людина не здатна відрізнити фейк від правди... все це марно. Тому цей рівень присвячений освітнім програмам з медіаграмотності. Розвитку критичного мислення. Суть — зміцнити не лише системи. А й свідомість.

Таблиця 1. Структура трирівневої архітектури інформаційного захисту

Рівень архітектури	Ключове завдання	Інструменти та методи	Цільова аудиторія / Учасники
1. Аналітичний (Технологічний)	Бачити загрозу раніше за всіх. Перетворювати інформаційний шум на чіткі сигнали.	Технологічний щит. Системи AI, що навчені відловлювати фейки. Інформаційні барометри... вони бачать аномалії раніше за людей. І, звісно, платформи для швидкої перевірки фактів.	Аналітичні центри; державні органи безпеки; спеціалізовані ІТ-компанії.
2. Комунікаційний (Організаційний)	Відповідати. Швидко. Скоординовано. Формувати єдине поле довіри.	Єдині координаційні центри... це мозок операції. Жорсткі протоколи, щоб усі говорили одним голосом. І, так, альянси. З медіа. З ІТ-гігантами.	Журналісти; лідери думок; представники влади; громадські організації.
3. Когнітивний (Соціальний)	Зміцнити суспільство. Створити колективний імунітет до маніпуляцій.	Медіаграмотність для всіх... і так, не лише для школярів. Практичні тренінги, що вчать бачити маніпуляції. І кампанії. Прості. Про інформаційну гігієну.	Широкі верстви населення: від школярів до літніх людей.

Ефективність та міжнародне значення: від локального досвіду до глобального стандарту

Ця модель, як стверджує автор, вже проходила випробування. Під час масованих інформаційних атак у Східній Європі прототипи такої системи показали надзвичайну ефективність.

І досвід довів... ключ до стійкості — не в цензурі. А в координації. Довірі. Та освіті. Запропонована модель дозволяє об'єднати зусилля держави, приватного сектору та громадянського суспільства.

А що далі? А далі — світ. У міжнародному контексті ця методика може бути легко адаптована. В рамках місій ООН та ЄС. В системі раннього попередження криз НАТО. І в освітніх програмах. Застосування цієї моделі є особливо актуальним для країн, що переживають постконфліктне відновлення.

Таблиця 2. Порівняльний аналіз ефективності протидії дезінформації

Параметр реагування	Традиційний підхід ("До")	Підхід на основі архітектури ("Після")	Ключова перевага
Виявлення загрози	Постфактум. Реакція на вже поширений фейк. Коли "пожежа" вже палає.	Проактивне. AI-системи бачать аномалії на ранніх стадіях. Ще до того, як фейк стане вірусним.	Перехоплення ініціативи. Ми не наздоганяємо. Ми діємо на випередження.
Координація відповіді	Хаотична. Кожне відомство дає свої коментарі. Часто суперечливі. Створюючи ще більше шуму.	Синхронізована. Єдиний координаційний центр. Єдиний, узгоджений меседж.	"Один голос". Це вбиває невизначеність і руйнує основу для маніпуляцій.
Робота з населенням	Пасивна. "Не панікуйте". Заклики, які ніколи не працюють. Люди залишаються сам на сам з потоком брехні.	Активна. "Ось факти. Ось інструкції. Ось як перевірити". Освітні програми створюють "імунітет".	Стійкість. Суспільство перетворюється з об'єкта атаки на активного учасника захисту.
Ефективність	Низька. Спростування завжди наздоганяє. Воно слабше за яскравий фейк.	Висока. Ми не спростовуємо. Ми випереджаємо, ізолюємо і маргіналізуємо дезінформацію.	Зміна правил гри. Ми перестаємо грати за правилами, які нам нав'язують.

Висновки

Запропонована трирівнева архітектура — це не просто ще один набір інструментів. Це, по суті, нова філософія стійкості. Автор доводить, що в інформаційній епосі більше не можна грати в обороні, нескінченно спростовуючи фейки, які з'являються швидше, ніж гриби після дощу. Потрібно діяти на випередження. Потрібно створювати "колективний імунітет" суспільства, де вірус дезінформації просто не зможе знайти собі поживного середовища.

Сила цієї моделі, як стверджує автор, полягає саме в її комплексності. Технології без людей — сліпі. Люди без технологій — безсилі. А всі вони без скоординованої комунікації — просто натовп. Лише синергія цих трьох рівнів

— аналітичного, комунікаційного та когнітивного — здатна перетворити розрізнені зусилля на єдиний, міцний інформаційний щит.

Звісно, це лише початок. Це креслення, а не збудована фортеця. Подальші розвідки мають зосередитися на практичних аспектах впровадження. Як адаптувати цю модель до різних культурних та політичних реалій? Як розробити універсальні метрики для вимірювання "когнітивного імунітету"? І як створити міжнародні "червоні лінії", правила гри в інформаційному просторі, які б стали загальновизнаними?

Відповіді на ці питання ще належить знайти. Але шлях вже визначено. Автор переконаний, що майбутнє безпеки — це не про будівництво стін. А про зміцнення свідомості. Це перехід від оборони до проактивного формування здорового, стійкого та критично мислячого інформаційного простору.

Література

1. Singer P. W., Brooking E. T. LikeWar: The Weaponization of Social Media. Houghton Mifflin Harcourt, 2018. 416 p.

2. Le Bon G. The Crowd: A Study of the Popular Mind. Dover Publications, 2002 (reprint). 144 p.

3. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. 4th ed. Pearson, 2020. 1136 p.

4. O'Neil C. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown, 2016. 272 p.

5. Rid T. Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux, 2020. 576 p.

6. Pomerantsev P. This Is Not Propaganda: Adventures in the War Against Reality. PublicAffairs, 2019. 256 p.

7. Kahneman D. Thinking, Fast and Slow. Farrar, Straus and Giroux, 2011. 512 p.

8. NATO Strategic Communications Centre of Excellence. Deterring Disinformation: A Guide to Proactive Communications. Riga : NATO StratCom COE, 2021.