ISSN 2522-1272
online ISSN 2786-8532

Scientific Notes of the Institute of Journalism, Vol. 88 (1) 2026

Journal homepage: https://nz.knu.ua/

Strategic Communications

https://doi.org/10.17721/2522-1272.2026.88.16

Asymmetric Tools of Influence and Strategic Communication in Cyberspace during the Russian-Ukrainian Full-Scale War

Yurii Havrylets, Dariia Anokhina
Taras Shevchenko National University of Kyiv, Ukraine

The article explores the phenomenon of asymmetry within the system of strategic communications in the context of modern cyber warfare. The authors categorize asymmetric tools, identifying cognitive, technological, and intelligence-informational methods of influence. Particular attention is paid to the communicative effects arising from the use of non-linear digital strategies: from civilian OSINT to algorithmic narrative management. It is proven that the full-scale war has triggered a transformation of StratCom models from hierarchical to networked ones, where the state acts as a moderator of a meaning-based ecosystem, and citizens become active subjects of cyber-resistance. It is substantiated that the use of asymmetric tools not only negates the adversary's resource advantage but also directly strengthens the cognitive resilience of society. The research *findings* can be applied to improve national security strategies and develop innovative approaches to information management in conflict environments.

Keywords: strategic communications, asymmetric influence, cyberspace, narrative management, cognitive resilience, network-centric warfare, OSINT, Russian-Ukrainian war

Citation: Гаврилець Ю., Анохіна Д. (2026). Асиметричні інструменти впливу та стратегічних комунікацій у кіберпросторі під час російсько-української повномасштабної війни. *Наукові Записки Інституту Журналістики*, *88*(1), 195–207. https://doi.org/10.17721/2522-1272.2026.88.16.

ISSN 2522-1272
online ISSN 2786-8532

Наукові записки Інституту журналістики, Том 88 (1) 2026

вебсайт журналу: https://nz.knu.ua/

Стратегічні комунікації

Асиметричні інструменти впливу та стратегічних комунікацій у кіберпросторі під час російсько-української повномасштабної війни

Юрій Гаврилець, Дарія Анохіна
Київський національний університет імені Тараса Шевченка, Україна

У статті досліджено феномен асиметрії в системі стратегічних комунікацій у контексті сучасної кібервійни. Автори здійснюють типологізацію асиметричних інструментів, виокремлюючи когнітивні, технологічні та розвідувально-інформаційні методи впливу. Основну увагу приділено комунікаційним ефектам, які виникають внаслідок застосування нелінійних цифрових стратегій: від цивільного OSINT до алгоритмічного управління наративами. Показано, що повномасштабна війна спричинила трансформацію моделей комунікацій у кіберпросторі від ієрархічних до мережевих, де держава виступає модератором екосистеми сенсів, а громадяни – активними суб'єктами кібервійни. Обґрунтовано, що використання асиметричних інструментів не лише нівелює ресурсну перевагу противника, а й безпосередньо зміцнює когнітивну стійкість власного суспільства. *Результати* дослідження можуть бути використані для вдосконалення стратегій національної безпеки та розробки новітніх підходів до управління інформаційними процесами в умовах конфлікту.

Ключові слова: стратегічні комунікації, асиметричний вплив, кіберпростір, управління наративами, когнітивна стійкість, мережецентрична війна, OSINT, російсько-українська війна

Повномасштабна збройна агресія РФ проти України остаточно закріпила статус кіберпростору як повноцінного середовища ведення війни, де межа між технологічним впливом та ментальним протистоянням стає дедалі чіткішою. У сучасних умовах стратегічні комунікації перестають бути лише інструментом супроводження кінетичних операцій, натомість вони перетворюються на самостійну силу, здатну визначати вектор політичних рішень та рівень суспільної стійкості (Дубов, 2014). Особливого значення у цьому контексті набуває феномен асиметрії, який дозволяє нівелювати кількісну чи ресурсну перевагу супротивника за рахунок інноваційних, нелінійних і при тому часто неформальних методів впливу.

Актуальність дослідження зумовлена тим, що російсько-українська війна стала першою війною такої інтенсивності, де асиметричні інструменти в кіберпросторі використовуються не епізодично, а системно – від децентралізованих ІТ-військ до алгоритмічного маніпулювання когнітивною вразливістю великих груп населення. Традиційні ієрархічні моделі державних комунікацій сьогодні змушені адаптуватися до мережевих структур, де

Юрій Гаврилець https://orcid.org/0000-0002-4899-5815
Дарія Анохіна https://orcid.org/0009-0009-3400-138X

Цю статтю було опубліковано спочатку онлайн 03 червня 2026 р. Вона є результатом дослідження кандидата наук із соціальних комунікацій, доцента кафедри соціальних комунікацій Юрія Гаврильця та студентки 2 курсу магістратури спеціалізації «Стратегічні комунікації» Дарії Анохіної у межах наукових тем кафедри соціальних комунікацій Київського національного університету імені Тараса Шевченка.

Автори заявляють про відсутність конфлікту інтересів. У розробленні дослідження, зборі, аналізі чи інтерпретації даних, у написанні рукопису спонсори участі не брали.

Кореспонденцію щодо цієї статті слід адресувати Юрію Гаврильцеві: **havrylets@knu.ua**.

ISSN 2522-1272
online ISSN 2786-8532

кожен користувач із доступом до мережі стає потенційним суб'єктом або об'єктом стратегічного впливу (Компанцева, Заруба, Череватий, Акульшин, 2022).

Наукова проблема полягає у необхідності переосмислення класичних підходів до управління наративами. Якщо раніше домінування в інформаційному полі забезпечувалося контролем над каналами поширення, то сучасна асиметрія в кіберпросторі базується на управлінні увагою, інтерпретаціями та емоційними станами аудиторії. У цьому плані не можемо не погодитися з тим, що комунікаційні ефекти таких інструментів виходять за межі віртуального простору, безпосередньо впливаючи на мобілізаційний потенціал суспільства, міжнародну підтримку та легітимізацію дій держави.

Звертаючись до поглядів науковців необхідно згадати і підхід Д. Дубова, який у своїй монографії доводить вже майже аксіоматичну гіпотезу: у сучасних умовах кіберпростір став інтегральним полем гібридного впливу, де атаки на інформаційну інфраструктуру поєднуються з інформаційними, психологічними та політичними операціями. Підхід науковця безпосередньо підтверджує та закріплює вже існуючі тези про кіберагресію як невід'ємний елемент гібридної війни (Дубов, с. 98–107).

Метою статті є ідентифікувати та систематизувати ключові асиметричні інструменти стратегічних комунікацій у кіберпросторі, а також аналіз їхніх комунікаційних ефектів у контексті повномасштабного протистояння між Україною і росією. *Об'єктом* дослідження є процеси формування та трансформації стратегічних наративів, а *предметом* – механізми використання нелінійних цифрових інструментів для досягнення цілей національної безпеки та оборони.

Теоретичне підґрунтя

Теоретична основа аналізу асиметричних інструментів у кіберпросторі будується на перетині теорії стратегічних комунікацій, концепцій мережевих війн та досліджень когнітивної безпеки. Вихідною точкою є розуміння стратегічних комунікацій як цілеспрямованого використання комунікації організацією для виконання її стратегічної місії, що було ґрунтовно досліджено у праці J. Hallahan, D. Holtzhausen та B. van Ruler (2007). У контексті безпекового сектору цей підхід доповнюється концепцією «комунікації як зброї» (Rid, 2012), де інформація стає ключовим інструментом примусу та впливу.

Закономірним є й факт наявності декількох сутнісних ознак кіберагресії, що посилюють її можливості впливу та ураження на арені гібридної війни. По-перше, її вирізняє асиметричність, яка здатна викликати дисонанс: не важливо, наскільки значними та потужними ресурсами володіє суперник, будь-який актор може завдати йому значної шкоди шляхом використання вразливостей його цифрової інфраструктури. По-друге, кіберагресію характеризує латентність. Джерело атаки почасти не є таким однозначним, що неабияк ускладнює політичну та правову відповідь у ході баталій. По-третє, неможливо уявити кіберагресію без масштабованості та високої швидкості реалізації. Почасти однієї атаки буде достатньо для синхронного різнорівневого впливу, що може охоплювати державне управління, фінанси, енергетику, транспорт і медіа. По-четверте, вплив кіберагресії не є прямим, що може вказувати як на досягнення безпосереднього технічного ефекту, так і вторинного політичного чи психологічного результату (Molander, Riddile, & Wilson, 1996).

Феномен асиметрії у сучасному протистоянні спирається на теорію «війн четвертого покоління» (4GW), описану W. Lind (2004), де акцент зміщується від фізичного знищення противника до розмивання його внутрішньої легітимності та волі до опору. Розвиток цієї думки у цифровому вимірі представлений у концепції «мережецентричної війни» (D. Alberts, J. Garstka, F. Stein, 2001), яка пояснює, як інформаційна перевага та горизонтальні зв'язки дозволяють малим групам ефективно протидіяти великим ієрархічним структурам.

ISSN 2522-1272
online ISSN 2786-8532

Соціально-комунікаційні ефекти кібервпливу розглядаються крізь призму теорії «інформаційного каскаду» та «ехо-камер», розроблених C. Sunstein (2017), що пояснюють механізми фрагментації суспільства та радикалізації наративів. Питання управління наративами в умовах цифрової асиметрії неможливо розглядати без праці A. Miskimmon, B. O'Loughlin, & L. Roselle, (2013) про стратегічні наративи як інструмент формування світового порядку.

Українська наукова думка зробила значний внесок у дослідження гібридних загроз. Роботи В. Горбуліна (2017) та Г. Почепцова (2015) закладають основу для розуміння стратегічного виміру інформаційних операцій, зокрема в контексті російської агресії. Питання медіатизації війни та ролі соціальних платформ як інструментів впливу детально аналізуються у дослідженнях Є. Магди (2015) та О. Курбана (2016).

Звертаючись до поглядів науковців, окремо відзначити слід підхід Д. Дубова, який у своїй монографії доводить вже майже аксіоматичну гіпотезу: у сучасних умовах кіберпростір став інтегральним полем гібридного впливу, де атаки на інформаційну інфраструктуру поєднуються з інформаційними, психологічними та політичними операціями. Підхід науковця безпосередньо підтверджує та закріплює вже існуючі тези про кіберагресію як невід'ємний елемент гібридної війни (Дубов, 2014, с. 98–107).

Критичне значення для розуміння асиметрії в кіберпросторі мають концепції «когнітивної війни» та «хакінгу людського сприйняття», які розглядають B. Claverie та F. du Cluzel (2023). Вони стверджують, що в сучасному конфлікті об'єктом атаки є не стільки дані, скільки мозок людини. Доповнюють це дослідження P. Singer та T. Brooking у праці «LikeWar» (2018), де аналізується, як соціальні медіа перетворили увагу на стратегічний ресурс.

Нарешті, методологія аналізу стійкості (resilience) перед обличчям асиметричних атак базується на підходах J. Nye щодо «м'якої сили» (2004) та сучасних звітах NATO Strategic Communications Centre of Excellence (NATO StratCom COE, 2023), які систематизують досвід протидії дезінформації в умовах кіберпростору.

Аналіз напрацювань вітчизняних та закордонних дослідників демонструє, що концептуальна рамка стратегічних комунікацій зазнала суттєвої еволюції: від класичного інформування до складних моделей управління когнітивними станами в умовах цифрової асиметрії. Проте, попри наявність ґрунтовної бази, більшість теоретичних моделей описують ієрархічні структури, тоді як досвід російсько-української війни вказує на виникнення динамічного симбіозу державних та мережевих суб'єктів. Це створює певний науковий розрив між класичним розумінням страткому як прерогативи державних інституцій та реальною практикою децентралізованого кіберопору, де асиметрія стає не просто тактичним прийомом, а новою стратегічною парадигмою.

Необхідність заповнення цієї лакуни та переосмислення соціально-комунікаційних механізмів впливу в умовах високоінтенсивного конфлікту зумовлює логіку нашого подальшого аналізу. Фокусуючись на переході від суто технологічного до соціально-поведінкового виміру кіберпростору, ми прагнемо не лише систематизувати наявний інструментарій, а й з'ясувати, як він трансформує архітектуру управління сенсами. Враховуючи вищевикладене, логіка дослідження базуватиметься на пошуку відповідей на такі ключові запитання:

RQ 1: Якою є типологія та функціональна специфіка асиметричних інструментів впливу, що застосовуються в кіберпросторі під час російсько-української повномасштабної війни?

Відповідь на це запитання дозволяє систематизувати такі інструменти та виявити їхні спільні риси як засобів стратегічної комунікації.

RQ 2: Яким чином використання асиметричних інструментів впливу трансформує класичні моделі управління стратегічними наративами (від ієрархічних до мережевих)?

ISSN 2522-1272
online ISSN 2786-8532

Тут критично важливим є теоретичний зсув – як «горизонтальні» цифрові зусилля (волонтери, ІТ-армія) інтегруються в державний стратком і як це впливає на швидкість та гнучкість формування наративів.

RQ 3: Які ключові комунікаційні ефекти (зокрема вплив на суспільну стійкість та когнітивну безпеку) спричиняє застосування асиметричних інструментів у кіберпросторі?

Це питання спрямоване на аналіз результатів: як ці інструменти змінюють поведінку аудиторії, рівень довіри до інституцій та здатність суспільства чинити опір інформаційній агресії.

Метод

Для досягнення мети дослідження та пошуку відповідей на поставлені запитання було застосовано комплексний методологічний підхід, що базується на принципах системності та міждисциплінарності. Дослідження реалізовано у межах соціально-комунікаційного підходу з використанням інструментарію теорії стратегічних комунікацій.

1. Теоретичні методи

На першому етапі було застосовано метод критичного аналізу наукової літератури та нормативної бази у сфері кібербезпеки та стратегічних комунікацій. Це дозволило концептуалізувати поняття «асиметрії» в кіберпросторі та виокремити його ключові характеристики порівняно з класичними методами інформаційного впливу. Використання компаративного методу дозволило порівняти тактики управління наративами, що застосовувалися на початкових етапах агресії, із сучасними мережецентричними моделями.

2. Емпіричні методи

Для ідентифікації та систематизації асиметричних інструментів (RQ1) та аналізу їхніх ефектів (RQ2, RQ3) було використано такі методи:

Метод кейс-стаді (Case study): Проаналізовано низку знакових подій у кіберпросторі протягом 2022–2026 років (наприклад, кампанії з використанням діпфейків, координація ІТ-армії). Це дало змогу детально розглянути механіку реалізації асиметричних стратегій у реальному часі.

Контент-аналіз та інтент-аналіз: Застосовувалися для дослідження повідомлень у соціальних медіа (Telegram, X, TikTok). Аналіз був спрямований на виявлення прихованих інтентів (намірів) комунікаторів, а також трансформації стратегічних наративів у процесі їхньої адаптації до цифрового середовища.

Моніторинг соціальних медіа (Social Media Intelligence): Для оцінки комунікаційних ефектів було проведено спостереження за динамікою залученості аудиторії та поширення вірального контенту, що дозволило зафіксувати зміни у суспільних настроях та рівні когнітивної стійкості.

3. Аналітичні процедури

Систематизація інструментів (RQ1) здійснювалася шляхом типологізації, що дозволило групувати методи впливу за функціональним призначенням (когнітивні, технологічні, OSINT-інструменти тощо). Аналіз трансформації моделей управління (RQ2) базувався на структурно-функціональному методі, який допоміг простежити перехід від централізованих до децентралізованих форм комунікації.

Результати та обговорення

У науковому дискурсі інформаційна війна здебільшого позиціонується як сплетіння різних форм впливу, що застосовуються одночасно або послідовно для дестабілізації

ISSN 2522-1272
online ISSN 2786-8532

держави-супротивника. Починаючи з військових дій та закінчуючи інформаційними кампаніями – головною характеристикою інструментарію залишається відсутність чітких меж між миром і війною. Ця логіка є винятковою для кіберагресії, так як дозволяє здійснювати вплив без прямого силового зіткнення, зберігаючи водночас високий рівень ефективності та складність атрибуції. Таким чином, створюється сприятливе підґрунтя для дестабілізації, послаблення інституційної спроможності держави та формування атмосфери невизначеності (Картунов, Маруховський, 2012).

Яскравим прикладом можна вважати кібератаку на супутникову мережу Viasat (KA-SAT) 24 лютого 2022 року, яка відбулася за кілька годин до початку повномасштабного вторгнення рф в Україну[1]. Технічною метою атаки було виведення з ладу тисяч супутникових модемів для обмеження можливості зв'язку Збройних сил України у критичний момент. Стратегічна ціль була дещо глибша – вона полягала у створенні так званої "інформаційної тиші" для ускладнення координації дій та створення атмосфери хаосу для дезорієнтації військових та цивільного населення. Так, згаданий інцидент є влучним підтвердженням методик поєднання технічного та комунікаційного ефектів кіберагресії навіть на ранньому етапі конфлікту.

Тож невелика кібероперація в одному сегменті мережі має на меті призвести до стратегічного засліплення військ та дезорієнтації цивільних у масштабах країни в критичні перші години вторгнення.

Ключовою характеристикою кіберагресії в умовах гібридної складової повномасштабної війни є дуалістична природа такої агресії. Маючи можливість одночасного впливу як на функціонування інфраструктури, так і на інформаційне середовище, вона здатна встановлювати власні правила гри. Найчастіше таку властивість можна спостерігати під час атак на критичні системи, де фізичний або технічний ефект доповнюється психологічним впливом. Так, наприклад, варто згадати кібератаку у квітні 2022 року, коли за допомогою шкідливого програмного забезпечення Industroyer2 ворог намагався вивести з ладу енергетичну інфраструктуру України. У разі успішного проведення кібероперації, окрім відключення електроенергії, противник досягнув би й значного психологічного тиску на населення – особливо в умовах війни, коли стабільність базових сервісів є критично важливою[2].

Цей кейс являє собою яскравий приклад інструментів, які б'ють по технічній системі, але мають основною ціллю «ментальну інфраструктуру» суспільства. Енергетичний колапс використовується як важіль для підриву довіри до держави («держава не може забезпечити базові потреби»), що є дешевшим та ефективнішим за масштабні ракетні обстріли для деморалізації тилу.

Схожа синергія простежується і в довготривалих кампаніях дезінформації, які супроводжують кібероперації. Тут варто згадати інцидент з кампанією «Doppelgänger» (2022–2024 рр.), ключовим завданням якої стало створення росією копій авторитетних європейських медіа з метою поширення фейкових матеріалів. Цей випадок наочно продемонстрував ефективність поєднання технічних інструментів (зокрема маніпуляцій з доменами та інфраструктурою) з інформаційним впливом, де кіберагресія була першочергово спрямована не на руйнування систем, а на підрив довіри до міжнародної

[1] ЄС звинуватив росію у зламі супутників Viasat за годину до вторгнення в Україну (2022). Суспільне Новини, 10.05.2022. https://suspilne.media/237923-es-zvinuvativ-rosiu-u-zlami-suputnikiv-viasat-za-godinu-do-vtorgnenna-v-ukrainu/.

[2] CERT-UA відбила російську кібератаку на енергетичний сектор України (2022). NV Техно. 12.04.2022. https://techno.nv.ua/ukr/it-industry/cert-ua-vidobrazila-rosiysku-kiberataku-na-energetichniy-sektor-ukrajini-50233159.html.

ISSN 2522-1272
online ISSN 2786-8532

підтримки України та формування альтернативної реальності в інформаційному просторі[3]. У результаті бачимо використання інструментів імітації для делегітимізації джерел правди та демократичних процесів. Використання авторитету відомих брендів чи голосів політиків проти них самих. Це створює «альтернативну реальність», де факт іноді дуже важко відрізнити від фікції.

У зв'язку з сучасними подіями, неабиякої ваги набуває і впровадження інструментів та механізмів кіберагресії з метою впливу на демократичні процеси. Так, проведення масованих атак на державні інформаційні системи під час виборів у європейських країнах, підкріплені розповсюдженням фейкових аудіозаписів політиків, наочно демонструють жагу до отримання керма влади не лише над інфраструктурою противника, але й над легітимністю політичних інститутів та результатами волевиявлення громадян[4]. Такий сценарій лише доводить ефективність інструментарію кіберагресії для підриву демократичних засад будь-якої держави. Тому як двокомпонентна модель комунікації П. Лазарсфельда (посилання) показує підсилення ретрансляції меседжів через лідерів думок та інфлюенсерів, ця ж модель може бути дуже дієвою у плані інформаційного очорнення чи знищення ключових політиків, громадських діячів та навіть моральних інститутів у суспільстві.

Але за допомогою асиметричних інструментів вплив ведеться не лише на великі соціальні групи. Зараз в умовах цифровізації дедалі частіше використовується таргетована кіберагресія, спрямована проти однієї особи чи вузької групи осіб для прямого психологічного тиску. Наприклад, операції з масової розсилки повідомлень військовим і їхнім родинам із погрозами або дезінформацією є наочним підтвердженням персоналізованого характеру сьогоденного впливу. У грудні 2023 р. через месенджер Signal, який вважається найзахищенішим у світі, українські військові та цивільні особи почали масово отримувати привітання російською мовою з Новим роком від невідомих акаунтів. У тексті йшлося про таке: «Нехай кожен із Вас з гордістю та трепетом підніме над головою російський триколор – символ державності, свободи та незалежності!»[5]. Цей інцидент змусив українське суспільство засумніватися в безпечності користування таким засобом зв'язку, як Signal. Із цього кейсу проявляється вихід сучасних конфліктів на вищий – когнітивний рівень, де ключовим об'єктом впливу стає свідомість.

Тому до масових атак на системи інфраструктури додався точковий вплив на людину як носія поведінкових реакцій. Пряме втручання у приватний цифровий простір особи та мінімальні витрати на SMS-шлюзи дають максимальний ефект індивідуального страху та деморалізації конкретних підрозділів.

Протягом повномасштабного вторгнення росії в Україну відбувалися атаки на цивільні сервіси, які не мають прямого воєнного значення, але визначають комфорт і відчуття безпеки в повсякденному житті. Як приклад, у грудні 2023 року була проведена потужна атака на одного з найбільших телеком-операторів України – «Київстар», що викликала суттєві проблеми зі зв'язком для мільйонів користувачів. Кіберінцидент спричинив масштабні наслідки, охопивши не лише комунікаційну складову, але й вразивши

[3] Півторак О. (2024). Операція «Doppelganger»: два роки антиукраїнської пропаганди. Детектор Медіа. https://detector.media/propahanda_vplyvy/article/231753/2024-09-05-operatsiya-doppelganger-dva-roky-antyukrainskoi-propagandy/.

[4] Російські боти спричинили різкий сплеск дезінформації в Х напередодні виборів у Німеччині (2024). Politico / Суспільне Новини. 20.12.2024. https://suspilne.media/943175-rosijski-boti-spricinili-rizkij-splesk-dezinformacii-v-h-naperedodni-viboriv-u-nimeccini-politico/.

[5] Українські військові отримують «новорічну» спам-розсилку від росіян у Signal: що каже розвідка (2023). Kyiv Post. 29.12.2023. https://www.kyivpost.com/uk/post/26097.

ISSN 2522-1272
online ISSN 2786-8532

функціонування систем оповіщення, банківських сервісів і повсякденного життя громадян[6]. У наведеному випадку, кіберагресія створила ефект “тотальної вразливості”, який за сприяння інформаційного резонансу здатен підірвати довіру до цифрової інфраструктури держави. Що дає агресору такий інструмент? Порушення звичного побуту людей (банкінг, логістика, зв’язок) створює відчуття «всюдисущості» загрози. Це асиметрична відповідь на цифровізацію держави: чим вищий рівень сервісів, тим більша потенційна ширина фронту для атаки.

Аналогічна логіка простежується і в атаках на логістичні системи, зокрема інциденті з “Новою Поштою” у 2024 році, який тимчасово дестабілізував функціонування ключового елементу внутрішньої економіки та волонтерських ланцюгів[7]. Метою кіберагресії стало порушення повсякденних процесів, що майстерно формує відчуття нестабільності та “всюдисущості” загрози у суспільних настроях.

Сьогоденні реалії диктують нові правила гри, де не останню роль відіграє використання штучного інтелекту для масштабування інформаційного впливу. Застосування великих мовних моделей для створення бот-мереж (операція «Matryoshka») спрямоване на масштабування генерації “реального” контенту, який складно відрізнити від публікацій справжніх користувачів[8]. Створюючи ілюзію суспільної думки, що може впливати на політичні процеси та громадські настрої (Microsoft Threat Intelligence), кіберагресія переходить на якісно новий рівень поширення впливу – автоматизованого управління інформаційним середовищем[9]. Асиметричність цього інструменту – у заміні тисяч «тролів» єдиним алгоритмом штучного інтелекту, що створює ілюзію масової підтримки чи протесту. Це дозволяє здійснювати масштабне «коригування поведінки» цільових аудиторій без залучення людського ресурсу.

Таким чином, підсумовуючи наведені вище кейси, можна констатувати факт функціонування кіберагресії у сучасній війні як інтегрованого інструмента впливу, який вміло поєднує в собі технічні, інформаційні та психологічні компоненти. Її ефективність визначається здатністю створювати синергетичний ефект, де кожен окремий елемент підсилює інший. Адже кіберагресія спрямовує свій потенціал не тільки на порушення функціонування систем, а й на створення умов для довготривалої дестабілізації та коригування поведінки цільових аудиторій, що є важливими факторами ведення будь-якої сучасної війни.

Беручи до уваги причинно-наслідкові чинники, що підтверджуватимуть нерозривність кіберагресії та гібридної війни, варто першочергово згадати про асиметричну природу першої, що дозволяє досягати значного ефекту при відносно менших витратах, та про чудову сумісність із іншими гібридними інструментами – дезінформацією, політичним тиском, економічним впливом, психологічними операціями. Не менш важливим є й ефект невизначеності, який є одним із головних механізмів гібридного протистояння, та середовище впливу, яке, порівняно з іншими елементами гібридної війни, є винятковим – це здатність кіберагресії впливати не лише на системи, але й на смисли, довіру та сприйняття (Дубов, 2014).

У цьому контексті традиційні підходи до протидії кіберагресії, зосереджені виключно на технічному захисті, є очевидно недостатніми. Навіть за умови ефективного усунення

[6] Хакери зруйнували частину IT-інфраструктури «Київстару» (2023). Коли планують відновити зв’язок (оновлюється). DOU. 13.12.2023. https://dou.ua/lenta/news/kyivstar-cyber-attack-restoration/.
[7] Обережно: кібератака! (2024). Нова пошта: офіційний сайт. https://novaposhta.ua/caution-cyber-attack/.
[8] Кремлівська мережа ботів «Матрешка» поширює фейки про розслідування справи Міндича в Україні (2025). Mind.ua. 21.11.2025. https://mind.ua/news/20297656-kremlivska-merezhi-botiv-matroshka-poshiryue-fejki-pro-rozsliduvannya-spravi-mindicha-v-ukrayini.
[9] Microsoft Defender Threat Intelligence (2026): Microsoft: official site. https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-threat-intelligence.

ISSN 2522-1272
online ISSN 2786-8532

технічних наслідків атаки, її інформаційний та психологічний ефект може зберігатися, впливаючи на довіру до держави та її інституцій.

Таким чином, фактично можна наголосити на інтегральності кіберагресії як важливого елемента гібридної складової сучасної війни, що функціонує на перетині безпекового та комунікаційного вимірів. Вміло інтегруючи різні форми впливу та досягаючи комплексного ефекту дестабілізації, кіберагресія займає важливу нішу у ході перебігу сучасних конфліктів. Водночас, надзвичайно ефективно протидіяти їй можна за допомогою застосування стратегічних комунікацій, які виступають не лише як інструмент реагування, але і як механізм формування стійкості держави та суспільства в нинішніх умовах.

Якою ж є реакція стратегічних комунікацій України на кіберзагрози від країни-агресора?

Загалом стратегічні комунікації є важливим для дослідження виміром національної системи кібербезпеки. Вони не лише виконують роль надання інформаційної підтримки державній політиці, а й відіграють важливу роль у встановленні стійкості проти руйнувань і зловмисних дій, підтриманні довіри до інституцій, координації відносин між акторами сектору безпеки та виступають противагою до наслідків, що виникають внаслідок інформаційно-психологічних операцій.

Таким чином, стратегічні комунікації – це комплексна багаторівнева система, що інтегрує різні інструменти впливу та забезпечує управління інформаційним середовищем у контексті національної безпеки. Їх теоретико-концептуальні засади висвітлюють їх як механізм смислового формування, координації дій та забезпечення стійкості суспільства, створюючи підґрунтя для подальшого аналізу їхньої ролі як інтегрального інструменту протидії інформаційним і кіберзагрозам у сучасному безпековому середовищі.

Показовою є історія української кампанії “Be brave like Ukraine”. Будучи, на перший погляд, брендинговою або іміджевою, в безпековому вимірі вона працювала як стратегічна комунікація високого рівня. Запропонувавши концентрований державний наратив “сміливості”, кампанія якісно поєднала внутрішню мобілізацію, зовнішню репрезентацію й психологічну стійкість. Проєкт був запущений урядом та Офісом Президента у 2022 році, тоді як ідея “bravery” була публічно закріплена Володимиром Зеленським як істинно українського бренду. Важливим нюансом є і безпекова функція кампанії. Знижуючи ефект нав’язаного Росією образу України як “жертви хаосу” і, натомість, формуючи образ суб’єктної, дієздатної та стійкої держави, кампанія зуміла сформувати влучний наратив, що став необхідним елементом національної стійкості[10].

Не варто забувати і про інноваційний проєкт “StopFake”, запущений викладачами, випускниками та студентами Києво-Могилянської школи журналістики 2 березня 2014 року. Долаючи звичні кордони фактчекінгу, “StopFake” вивело громадянське суспільство на новий етап, перетворивши його із зовнішнього спостерігача на структурний елемент системи стратегічних комунікацій. Основним завданням проєкту було не стільки спростування фейків про Україну, як створення культури розпізнавання маніпуляцій задля подальшого функціонування на рівні довгострокової інформаційної гігієни[11]. Так, можна побачити ще один “поверх” функціонування стратегічних відносин, що відбувається не через державу, а через мережу довірених недержавних акторів.

Зовнішній вимір значущості стратегічних комунікацій простежується на прикладі ініціативи “Grain from Ukraine”, яка якісно підкреслює глобальну роль України. Незважаючи на гуманітарну місію, вона охоплює і функцію стратегічної комунікації,

[10] The Power of Bravery: National Branding in Times of War (2024). Ukraine.ua ; Ministry of Foreign Affairs of Ukraine. https://ukraine.ua/success-stories/be-brave-like-ukraine/.
[11] StopFake: як працює найвідоміша в Україні ініціатива з фактчекінгу : веб-сайт (2017). MediaLab Online. https://medialab.online/news/stopfake/.

ISSN 2522-1272
online ISSN 2786-8532

демонструючи міжнародній аудиторії Україну не лише як об'єкт війни, але і як суб'єкт глобальної продовольчої безпеки. У контексті протидії інформаційним загрозам, ключові повідомлення ініціативи перетворюються на контрнаратив до російських меседжів про "українську нестабільність" або "непотрібність підтримки України". У контексті протидії інформаційним загрозам це працює як контрнаратив до російських закликів про "українську нестабільність" або "непотрібність підтримки України"; це демонструє роль стратегічних комунікацій як важливого інструменту геополітичного позиціонування[12].

Повертаючись до інтернаціонального контексту, на рівні міжнародних організацій показовою є практика НАТО. Підхід Альянсу до протидії інформаційним загрозам акцентує увагу на важливості відкритої та превентивної комунікації з метою мінімізації ефективності ворожих наративів. Кампанія #WeAreNATO ілюструє інший важливий аспект: стратегічні комунікації не є "одноразовим" інструментом, "ліками" від кризи; насамперед, їхнім покликанням є довгострокова легітимація безпекових інституцій у власних суспільствах. Так, мета кампанії полягала в тлумаченні внутрішнім аудиторіям країн-членів ролі НАТО поряд із підтримкою суспільного розуміння колективної оборони. Кампанія продемонструвала, що стійкість до загроз починається ще до самої кризи – із наявності довіри, зрозумілої місії та легітимної публічної присутності інституції[13].

Примітним у цьому плані є приклад Естонії після масштабних кібератак 2007 року. Згідно з дослідженнями Центру передового досвіду НАТО зі стратегічних комунікацій, ситуація є типовим випадком гібридної загрози, з характерними "додатками" до кібероперацій у вигляді залучення до політичних та комунікаційних процесів. Естонія зробила болючий, однак важливий висновок – відновлення систем саме по собі не є достатнім; критично важливими є координація уряду, IT-сектору, медіа та суспільства, а також робота над довгостроковою резильєнтністю[14]. Так, можна вкотре побачити підтвердження комплексного сприйняття стратегічних комунікацій – не лише як реагування на інцидент, а і як елементи архітектури національної стійкості.

Не менш важливим механізмом є превентивне інформування про можливі сценарії поширення дезінформації чи кіберпровокацій. Традиційно, на жаль, держава почасти звикла діяти постфактум – спростовувати вже поширений фейк або пояснювати вже реалізований інцидент. Превентивна комунікація виступає набагато ефективнішою завдяки поясненню суспільству про конкретні наративи або інформаційні маніпуляції, що можуть суспільству загрожувати, висвітленню їх способу та мети. Як наслідок, держава здатна мінімізувати ефект раптовості, розвинути у населення критичність сприйняття інформації, тим самим позбавивши агресора значної частини комунікативної переваги.

Яскравим прикладом згаданого механізму є стратегічні практики Тайваню. Підхід держави під назвою "Humor over Rumor" є дійсно ефективним знаряддям випереджувального інформування та нейтралізації фейків до їхнього масового поширення. І саме такі підходи формують "суспільний імунітет" до дезінформації, що є критично важливим у контексті когнітивної війни[15].

---

[12] Ініціатива Grain from Ukraine підкреслює глобальну роль України в гарантуванні продовольчої безпеки (2022). Президент : офіційне інтернет-представництво / Президент України Володимир Зеленський. https://www.president.gov.ua/news/iniciativa-grain-ukraine-pidkreslyuye-globalnu-rol-ukrayini-79473.

[13] #WeAreNATO: Strategic Communications, Engagement and Lessons Learnt (2021). Atlantic Forum. https://www.atlantic-forum.com/our-views/wearenato-strategic-communications-engagement-and-lessons-learnt.

[14] The 2007 Cyberattacks on Estonia: A Case Study in Hybrid Warfare and Strategic Communications : report (2024). NATO Strategic Communications Centre of Excellence. Riga. https://stratcomcoe.org/publications/the-2007-cyberattacks-on-estonia-lessons-learned/256.

[15] Humor over Rumor: Combating Disinformation around COVID-19 in Taiwan : analysis (2021). Global Governance Futures. https://www.ggfutures.net/analysis/humor-over-rumor-combating-disinformation-around-covid-19-in-taiwan.

ISSN 2522-1272
online ISSN 2786-8532

Зазвичай у межах кіберпростору стратегічні комунікації реалізуються через різні канали. До традиційних належать офіційні заяви органів влади, пресрелізи, брифінги, урядові сайти та офіційні сторінки інституцій. Однак в епоху цифровізації, безсумнівно, виникає запит на ширшу каналову архітектуру, – тому у "гру" вступають соціальні мережі, месенджери, мобільні застосунки, спеціалізовані платформи кризового інформування, офіційні канали безпекових структур, а також медіа-партнерства. Саме багатоканальність комунікації є запорукою охоплення різних аудиторій, зменшуючи ризик інформаційного розриву та дозволяючи адаптувати повідомлення до різних груп сприйняття під час виникнення кризової ситуації.

Не менш важливими є важелі впливу, за допомогою яких стратегічні комунікації досягають безпекового ефекту. Першочерговим та базовим елементом будь-якої комунікаційної взаємодії є, безперечно, довіра. Підкріплює попередній важіль наратив, який дозволяє не просто інформувати, а впорядковувати події у зрозумілу смислову рамку. Наступним важелем впливу є авторитет джерела, що за сутністю є інституційною легітимністю мовця. Четвертим важелем виступає швидкість реакції, яка визначає здатність держави першою задати рамку інтерпретації події. Останній, однак не менш важливий – повторюваність і узгодженість повідомлень, які формують стабільність сприйняття та знижують простір для маніпуляцій[16].

До слова, аналіз тенденцій за останні роки демонструє декілька ключових напрямів трансформації ролі стратегічних комунікацій у секторі безпеки та оборони України. По-перше, стає дедалі помітнішим збільшення синергії штучного інтелекту для генерації дипфейків, шкідливого коду, автоматизованих інформаційних кампаній та штучного моделювання суспільної думки. Безперечно, у відповідь на таку технологічну еволюцію, стратегічним комунікаціям необхідно пройти і власний етап трансформації, ключовим завданням якого є перехід до автоматизованих інструментів моніторингу, виявлення аномалій у наративному середовищі та швидкого реагування на нові форми маніпуляції. По-друге, важливим є і перехід від моделі пасивної стійкості до активного впливу, що перетворює стратегічні комунікації з інструменту захисту від ворожих наративів на інструмент формування сприятливого інформаційного середовища, посилення власних позицій та обмеження простору для агресора. По-третє, дедалі більшого значення набуває мережевість комунікації, коли державні, громадські та приватні суб'єкти діють не окремо, а в режимі багаторівневої координації.

Висновки

Доцільно виокремити триєдину модель функціонування стратегічних комунікацій у протидії сучасним кіберзагрозам. Перший рівень можна описати як технічний: він охоплює класичні інструменти кібербезпеки, такі як захист інфраструктури, виявлення та нейтралізацію атак, резервування систем, підтримання безперервності функціонування сервісів. Проте цей рівень не може сам по собі розв'язати проблему суспільного сприйняття інциденту. Другий рівень – рівень сенсів, передбачає управління суспільними реакціями, підтримання довіри до держави, зниження рівня паніки та формування стійкості до інформаційного тиску. Останній, третій рівень, націлений на управління суспільними реакціями, підтримання довіри до держави, зниження рівня паніки та формування стійкості до інформаційного тиску, що визначає його як психологічний. Лише за умови якісної

[16] Ten Years On: The Evolution of Strategic Communication and Information Operations since 9/11: Hearing before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services House of Repre- sentatives (2011). 112 Cong. (12 July 2011). H.A.S.C., 112–149. http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg67796/pdf/CHRG-112hhrg67796.pdf.

взаємодії цих трьох рівнів стратегічні комунікації можуть функціонувати як повноцінний механізм безпекового реагування.

Таким чином, можна стверджувати, що завершеного аналітичного осмислення кіберагресія як елемент гібридної війни набуває лише за умови проходження через призму механізмів стратегічних комунікацій. Останні є влучним поєднанням технічного, смислового і психологічного рівнів реакції, дозволяючи мінімізувати вразливість до інформаційних маніпуляцій, управляти наслідками інцидентів, зберігати довіру до держави та формувати суспільну стійкість. Сучасні конфлікти є показовим прикладом важливості повноцінної інтеграції стратегічних комунікацій у систему національної кібербезпеки задля ефективної протидії кіберагресії.

Також особливої уваги в сучасних умовах потребує феномен кіберсоціальної інженерії, який стає одним із найсерйозніших викликів для системи національної безпеки. Маніпуляція людським фактором стає вагомим інструментом реалізації кібератак, і може проявлятися через психологічний тиск, фішинг, імітацію офіційних джерел, нав'язування хибних рішень, або ж створення атмосфери страху. В такому випадку превентивність стратегічних комунікацій є вирішальним фактором, що допомагає вчасно трансформувати звичайне інформування у довгострокову модель поведінкової зміни. Так формується культура цифрової гігієни, основним об'єктом якої визначається кожен громадянин як активний елемент національного кіберщита.

Таким чином, поєднуючи у собі державне пояснення, кризову реакцію, превентивну роботу з аудиторіями, підтримку інституційної легітимності та захист інформаційного середовища, стратегічні комунікації перетворилися на інтегральний інструмент протидії інформаційним і кіберзагрозам в сучасному безпековому середовищі. Маючи змогу працювати не тільки з інцидентом, а й із його наслідками для свідомості, довіри та поведінки, стратегічні комунікації вже давно стали необхідною умовою ефективної кіберстійкості суспільства. Тому в наступних дослідженнях доцільно буде детальніше розглянути конкретні механізми стратегічних комунікацій у кіберпросторі, їхні канали реалізації, важелі впливу та практики застосування.

Декларація про генеративний штучний інтелект та технології, що використовують штучний інтелект у процесі написання. Під час підготовки цього рукопису не використовувалися інструменти штучного інтелекту для створення, написання або редагування тексту. Усі результати є оригінальними та отримані без допомоги ШІ.

Посилання

Alberts, D. S., & Garstka, J. J., & Stein, F. P. (2001). Network Centric Warfare. DoD Cooperative Research Program. http://dodccrp.org/files/Alberts_NCW.pdf.

Claverie, B., & du Cluzel, F. (2023). The Cognitive Warfare Concept. NATO Innovation Hub. https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf.

Hallahan, K., Holtzhausen, D., van Ruler, B., Verčič, D., & Sriramesh, K. (2007). Defining Strategic Communication. International Journal of Strategic Communication, 1(1), 3–35. https://doi.org/10.1080/15531180701285244.

Lind, W. S. (2004). Understanding Fourth Generation War. Military Review.

Miskimmon, A., O'Loughlin, B., & Roselle, L. (2013). Strategic Narratives: Communication Power and the New World Order. Routledge.

Molander, R. C., Riddile, A. S., & Wilson, P. A. (1996). Strategic information warfare: a new face of war. https://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR661.pdf

NATO StratCom COE. (2023). Social Media Manipulation Report. Riga.

Nye, J. S. (2004). Soft Power: The Means to Success in World Politics. PublicAffairs.

Rid, T. (2012). Cyber War Will Not Take Place. Oxford University Press.

ISSN 2522-1272
online ISSN 2786-8532

Singer, P. W., & Brooking, E. T. (2018). LikeWar: The Weaponization of Social Media. Eamon Dolan/Houghton Mifflin Harcourt.

Sunstein, C. R. (2017). #Republic: Divided Democracy in the Age of Social Media. Princeton University Press.

Горбулін, В. П. (2017). Світова гібридна війна: український фронт. НІСД.

Дубов, Д. В. (2014). Кіберпростір як новий об'єкт державної політики. НІСД.

Картунов О., Маруховський О. (2012). Інформаційне суспільство: аналіз політичних аспектів зарубіжних концепцій: Монографія. Київ: Університет економіки та права «Крок». 344 с.

Компанцева О., Заруба О., Череватий С., Акульшин О. (2022). Стратегічні комунікації для безпекових і державних інституцій : практичний посібник. Київ: ТОВ «ВІСТКА». http://fes.kiev.ua/n/cms/fileadmin/upload2/Book_28-06-2022_web-3.pdf.

Курбан, О. В. (2016). Інформаційні війни у соціальних мережах. КНУ.

Магда, Є. В. (2015). Гібридна війна: вижити і перемогти. Віват.

Почепцов, Г. Г. (2015). Сучасні інформаційні війни. Видавничий дім «Києво-Могилянська академія».

Received 15.05.2026
Approved 22.05.2026
Published 26.05.2026