Funded by the European Union

ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЛЕСІ УКРАЇНКИ
ФАКУЛЬТЕТ МІЖНАРОДНИХ ВІДНОСИН
КАФЕДРА МІЖНАРОДНИХ КОМУНІКАЦІЙ
ТА ПОЛІТИЧНОГО АНАЛІЗУ

ЗОВНІШНЄ ІНФОРМАЦІЙНЕ МАНІПУЛЮВАННЯ ТА ВТРУЧАННЯ В УМОВАХ СУЧАСНИХ КОНФЛІКТІВ

Збірник матеріалів інтернет-конференції

(Луцьк, 14 травня 2025 р.)

ЛУЦЬК-2025

УДК 323]:070.16:316.775.23(08)
З-78

Зовнішнє інформаційне маніпулювання та втручання в умовах сучасних конфліктів: матеріли інтернет-конференції / за заг. ред. проф. Н. Карпчук. – Луцьк: ВНУ імені Лесі Українки, 2025. – 215 с.

Рекомендовано вченою радою факультету міжнародних відносин
Волинського національного університету імені Лесі Українки
(протокол № 10 від 21 травня 2025 р.)

Рецензенти:

Тетяна Сидорук – доктор політичних наук, професор, завідувач кафедри міжнародних відносин, Національний університет «Острозька академія» (м. Острог).

Наталія Романюк – кандидат географічних наук, доцент кафедри міжнародних відносин та регіональних студій, експерт проектів Жана Моне, керівник Інформаційного центру ЄС, Волинський національний університет імені Лесі Українки

Матеріали інтернет-конференції опубліковано в рамках реалізації проєкту
ERASMUS+ JEAN MONNET MODULE
«Протидія ЄС зовнішньому інформаційному маніпулюванню та втручанню»
№ 101172342 – EUC2FIMI – ERASMUS-JMO-2024-HEI-TCH-RSCH

Фінансується Європейським Союзом. Проте висловлені погляди та думки належать лише авторам і не обов'язково відображають погляди Європейського Союзу чи Європейського виконавчого агентства з питань освіти та культури (EACEA). Ні Європейський Союз, ні EACEA не можуть нести за них відповідальність.

Представлені матеріали включають тези доповідей, що розкривають гібридну сутність сучасних конфліктів. Особливий акцент матеріалів на інструментах «гібридності»: зовнішньому інформаційному маніпулюванню та втручанню (FIMI), дезінформації, злісній діяльності у кіберпросторі, мілітарному компоненту. Збірник матеріалів є корисним для науковців, викладачів, студентів, представників органів державної влади та інститутів громадянського суспільства, які цікавляться питаннями зовнішнього інформаційного маніпулювання та втручання.

Матеріали подано в авторській редакції

ЗМІСТ

ГІБРИДНІ ЗАГРОЗИ Й ГІБРИДНІ КОНФЛІКТИ

ЗОВНІШНЄ ІНФОРМАЦІЙНЕ МАНІПУЛЮВАННЯ ТА ВТРУЧАННЯ (FIMI). ДЕЗІНФОРМАЦІЯ. ДЕСТРУКТИВНА ПРОПАГАНДА

систему, де лояльність купувалася через доступ до ресурсів та можливості збагачення. Саме такий підхід забезпечив довгостроковий вплив на регіон, доповнюючи військову присутність економічними важелями[19].

Особливу увагу приділяли соціальним виплатам та інфраструктурним проектам, які мали демонструвати «відновлення мирного життя». Однак, як зазначають дослідники, ці програми реалізовувалися вибірково, переважно в стратегічно важливих районах, створюючи видимість благополуччя. Паралельно формувалася система патронажу, коли доступ до соціальних благ залежав від політичної лояльності. Ця модель згодом була адаптована до інших регіонів, зокрема до окупованого Криму та частини Донбасу. Використання економічних стимулів дозволяло створювати ілюзію добровільного вибору населення на користь російської влади. При цьому ключові галузі економіки залишалися під контролем федерального центру, що забезпечувало довгостроковий вплив на регіон[20].

Російсько-чеченські війни стали ключовим етапом у розвитку сучасної гібридної війни. Перший конфлікт показав неефективність традиційних силових методів, але саме тоді почали формуватися основи нової стратегії – інформаційні операції, використання місцевих колаборціоністів і маніпулювання суспільною думкою. Під час другого конфлікту Росія вже діяла набагато витонченіше, поєднуючи військову силу з ретельно підготовленим приводом для вторгнення, повним контролем інформаційного простору, використанням проксі-сил та масштабними економічними програмами. Цей досвід став основою для подальших операцій у Грузії, Криму та на Донбасі, де було доведено, що ефективний контроль досягається не лише зброєю, а й комплексним поєднанням різних інструментів впливу, що дозволяє формувати бажану політичну реальність.

*****

Сергій Федонюк, кандидат географічних наук, доцент кафедри міжнародних комунікацій та політичного аналізу
Волинський національний університет імені Лесі українки

ОПЕРАЦІОНАЛІЗАЦІЯ VUCA В КОНТЕКСТІ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНИХ ЗАГРОЗ

Концепт VUCA утвердився в науковій і стратегічній термінології як евристична рамка для опису складної й нестабільної природи сучасного середовища. Водночас його прикладне застосування в контексті конкретних інформаційних криз залишається недостатньо розробленим. Загальні означення – на кшталт «мінливого середовища» чи «зростання

[19] Друга чеченська (2003). Видавництво "Український прес-клуб". 320 с.
[20] Економіка окупації: російські моделі контролю (2005). Видавництво Гарвардського університету. 385 с.

неоднозначності» – не дають відповіді на критичні запитання: *де саме*, *коли саме* та *чому саме* відбувається втручання у національний інформаційний простір.

Упродовж останнього десятиліття інформаційний простір, по суті, трансформувався на арену гібридних і конвенційних конфліктів, у якій стратегічні переваги досягаються не стільки за допомогою класичної пропаганди, як через складні багаторівневі інформаційні операції, що дедалі частіше використовують властивості середовища з характеристиками VUCA – волатильності (volatility), невизначеності (uncertainty), складності (complexity) та неоднозначності (ambiguity) – як інструментів дестабілізації[21].

Інформаційні кампанії нового покоління підривають довіру до державних інституцій (невизначеність), стимулюють емоційні коливання через дезінформаційні вкиди (волатильність), продукують конкуруючі наративи (неоднозначність), формують складні мережі ботів, псевдоекспертів і ретрансляторів (складність). Це суттєво ускладнює застосування класичних моделей протидії, зокрема систем перевірки фактів, які не встигають за швидкістю поширення інформації в цифровому середовищі.

Відповідь демократичних держав, включаючи інститути НАТО та ЄС, часто залишається реактивною, оскільки операції впливу базуються на властивостях самого інформаційного середовища:

–*Волатильність* (V): цифрові платформи, зокрема TikTok і Telegram, здатні формувати миттєві вірусні ефекти до того, як спрацюють механізми перевірки[22];

–*Невизначеність* (U): фрагментарність даних у перші години кризи змушує аудиторію керуватися емоційною реакцією замість раціонального аналізу[23];

–*Складність* (C): багатоходові наративи у транснаціональному середовищі перешкоджають простому встановленню джерел і маршрутів поширення інформації[24];

–*Неоднозначність* (A): конкуренція між різними фреймами інтерпретації подій (наприклад, «внутрішній протест» чи «зовнішнє втручання») веде до соціальної поляризації ще до появи офіційних комунікацій[25].

Особливо вразливими в таких умовах є молоді демократії, що перебувають у стані військової агресії, зокрема Україна в період 2022–2024 рр. Держави змушені оперативно

[21] Bennett, N., & Lemoine, G. J. (2014). What VUCA really means for you. *Harvard Business Review*, 92(1/2), 27.
[22] Saurwein, F., & Spencer-Smith, C. (2020). Combating Disinformation on Social Media: Multilevel Governance and Distributed Accountability in Europe. *Digital Journalism*, *8*(6), 820–841. https://doi.org/10.1080/21670811.2020.1765401
[23] Marwick, A., & Lewis, R. (2017). *Media Manipulation and Disinformation Online*. Data & Society Research Institute. https://datasociety.net/library/media-manipulation-and-disinfo-online/
[24] Kavanagh, J., & Rich, M. D. (2018). *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life*. RAND Corporation. https://doi.org/10.7249/RR2314
[25] Entman, R. M. (2008). Theorizing Mediated Public Diplomacy: The U.S. Case. *The International Journal of Press/Politics*, *13*(2), 87-102. https://doi.org/10.1177/1940161208314657 (Original work published 2008)

переглядати власну комунікаційну архітектуру – від тактичних інструментів типу чат-ботів до стратегічних механізмів дипломатичного інформування.

Окрему загрозу становить те, що ворожі актори активно інвертують VUCA-фактори, трансформуючи їх на інструменти атаки: генерують штучну волатильність через «інфошум», посилюють невизначеність за рахунок анонімних вкидів, ускладнюють інформаційний ландшафт через багаторівневі мережі, множать неоднозначність шляхом залучення псевдонаукових або маргінальних інтерпретацій.

Попри наявність розрізнених аналітичних підходів, сьогодні залишається відкритим питання про формалізоване спостереження та оцінювання VUCA-вразливостей у реальному часі. Зокрема, бракує уніфікованої системи метрик, які дозволили б кількісно фіксувати волатильність, фрагментацію, структурну складність і семантичну неоднозначність інформаційних потоків. Також не відомо про застосування відповідних індикаторів раннього попередження для урядових і наднаціональних структур та просторово-часових моделей картування зовнішнього впливу.

Тому дослідницька проблема у цьому аспекті полягає в необхідності операціоналізувати компоненти VUCA у параметрах мережевої аналітики (наприклад: *connection density, redundancy level, cognitive entropy, polarization index*), та, відповідно, створити динамічну модель картування зовнішніх втручань, при цьому сформулювавши набір прогностичних індикаторів інформаційної уразливості, здатних підтримати перехід від реактивних до проактивних стратегій безпеки.

Попередні спроби відстежувати інформаційні маніпуляції спиралися переважно на постфактум-аналіз окремих фейків або кібератак. Перенесення VUCA-рамки у вимірювані показники створює живий датчик, наприклад, ми бачимо, коли волатильність або неоднозначність досягають порога, за якого будь-який зовнішній «вкид» проривається крізь інформаційну «броню».

Метою є переклад абстрактної чотирикомпонентної моделі VUCA у формалізовану систему кількісних індикаторів, отримуваних у реальному часі з відкритих даних (соціальні мережі, новинні стрічки, бази подій), що дозволяє підживлювати системи раннього попередження у сфері інформаційної безпеки, наприклад:

Volatility (V) кількісно можна виразити через динаміку залученості аудиторії: час від інформаційного тригера до піку обговорення; амплітуда стрибків; ступінь плинності аудиторного складу. Показник максимальної волатильності (скажімо V = 5) фіксується, коли протягом двох годин після мінімального інформаційного імпульсу третина учасників дискурсу змінюється.

Uncertainty (U) інтерпретується не як «брак інформації», а як розрив між очікуванням і наявним знанням. Операціоналізацію можна здійснити через: частку суперечливих повідомлень у потоці; кількість запитів на перевірку фактів або підтвердження джерел. Зростання показника U фіксується зі збільшенням частоти звернень до верифікаторів («це точно?»).

Complexity (C) описує структурну заплутаність мережевої взаємодії. Індекс Cx = (1/L + CC)/2, де: *L* – середня довжина шляху в мережі; *CC* – коефіцієнт кластеризації.

Значення C = 4–5 буде властиве щільно зшитим, багаторівневим мережам, характерним для інформаційних атак із зовнішнім втручанням.

Ambiguity (A) визначається як множинність і конкуренція тлумачень подій. Відповідно, методологічно застосовується текстова фрейм-аналізова модель: визначається, яку частку корпусу охоплюють два домінантні наративні фрейми. Якщо ця частка менша 30 %, фіксується A = 5 – стан максимального семантичного туману.

Усі індикатори потрібно нормувати до інтервалу [0;1] та інтерпретувати у п’ятибальній шкалі (1–5 квінтилів).

Таким чином, основна гіпотеза полягає в тому, що розгляд VUCA-факторів як операціоналізованих змінних дасть змогу сформувати єдину евристичну рамку для діагностики, моделювання та управління інформаційними ризиками у контексті сучасних конфліктів.

*****

Діана Матраєва, студентка групи 4571 спеціальності К3 «Національна безпека (за окремими сферами забезпечення і видами діяльності)»
Миколаївський національний університет імені Адмірала Макарова (м. Миколаїв, Україна)

ГІБРИДНІ АСПЕКТИ СУЧАСНОЇ ВІЙНИ В СИРІЇ

Концепція гібридної війни стає дедалі актуальнішою у сучасних міжнародних відносинах. Традиційні форми збройної боротьби доповнюються інформаційними кампаніями, економічним тиском, кібератаками та залученням нерегулярних сил, що змінює уявлення про характер і динаміку воєнних конфліктів. Одним із найяскравіших прикладів гібридного конфлікту XXI століття є війна в Сирії.

Вона виникла в умовах внутрішньої політичної кризи, спричиненої авторитарною політикою уряду Башара Асада, однак дуже швидко набула масштабів складної регіональної та глобальної боротьби за вплив і ресурси. У сирійському конфлікті сплелися між собою різноманітні форми насильства, економічного блокування, пропаганди та психологічного