Демиденко В. О.,
кандидат юридичних наук, доцент, професор кафедри конституційного права та прав людини,
Національна академія внутрішніх справ
(м. Київ, Україна)

ГІБРИДНІ ЗАГРОЗИ СТІЙКОСТІ ДЕРЖАВНОГО ТА МУНІЦИПАЛЬНОГО УПРАВЛІННЯ В УМОВАХ ПЕРЕХОДУ ДО НИЗЬКОЇ ВОЄННОЇ ІНТЕНСИВНОСТІ

Четвертий рік поспіль триває широкомасштабне вторгнення російської федерації в Україну та її варварська, кривава збройна агресія, яка використовує комплекс конвенційних та терористичних засобів — від жорстокої військової наземної кампанії до масованих терористичних повітряних ударів. Ця агресія спрямована насамперед на незаконне захоплення українських територій, геноцидне знищення Українського народу та його ідентичності, а також на свідоме поширення внутрішнього хаосу в управлінні державою.

Водночас, за допомогою цієї війни російська федерація намагається досягти ще однієї людиноненависної глобальної мети. Це підірвати єдність і цілісність західної демократії у розумінні її цінностей та непохитному бажанні їх відстоювати, зруйнувати євроатлантичну єдність та зародити і посилити стратегічне протистояння між Європейським Союзом та Сполученими Штатами Америки.

Варто наголосити, що парадигма відносин між державами-членами НАТО суттєво змінилася. Фокус змістився з консолідованої співпраці в межах єдиного ціннісного коридору (права людини, верховенство права, демократія тощо) на банальний фінансовий вимір. Така зміна підходу є загрозливою, адже в умовах неминучих збройних конфліктів цивілізований світ ризикує бути розпорошеним, оцінюючи протистояння виключно з точки зору вигоди. Світ, де загальна міжнародна ціннісна площина страждає, приречений на низку конфліктів, які лише посилюватимуться, оскільки єдність авторитарних режимів, їхня жорсткість у підтримці один одного та готовність застосувати будь-яку зброю, включно з ядерною, не залишає сумнівів у їхній безкомпромісності.

Наразі підтримка з боку США потрібна Україні, європейським членам НАТО, державам-членам Європейського Союзу від російської агресії. Проте горизонт стратегічного планування вимагає оцінки завтрашніх загроз. З огляду на нинішній характер відносин між США та Китаєм, а також на глобальні економічні негаразди, що негативно впливають на ВВП обох країн, існує високий ризик ескалації. Військовий конфлікт за Тайвань — світового лідера у виробництві наночипів, які є основою цифрового зростання та штучного інтелекту — може стати виходом, що має знівелювати системні прорахунки з боку керівництва як Китаю, так і США. У цьому контексті виникає критичне

питання щодо ймовірної фундаментальної та достатньо рішучої підтримки Європейським Союзом Сполучених Штатів у протистоянні (не виключено і військовому) з Китаєм, якщо вже сьогодні ми спостерігаємо втрату спільного ціннісного фундаменту у відносинах між членами Альянсу.

Разом з тим російська агресія в Україні видозмінюється, оскільки в агресора вже нині спостерігається недостатність ресурсів для великих сухопутних наступальних операцій. А як відомо воєнні злочинці, що входять до вищого військово-політичного керівництва московії є прихильниками концепції «гібридної війни». Виходячи з аналізу бюджету російських окупантів на 2026 рік є обґрунтовані підстави для гіпотетичного припущення, що питома вага прямої військової агресії у загальній картині конфлікту може поступово знижуватися. Із виснаженням ресурсів та зміною стратегічного фокусу, війна може еволюціонувати у фазу низької інтенсивності, де прямі масштабні зіткнення заміняться некінетичними інструментами — високотехнологічними ударами, кіберпротистоянням та інформаційною конфронтацією, зберігаючи при цьому стійку напругу на лінії розмежування.

Як наслідок, виникає питання щодо готовності Української держави та народу до таких вже зараз вагомо зростаючих складових сучасної гібридної війни, як інформаційно-психологічна складова російської гібридної війни проти України, ЄС та загалом вільного світу. Остання спрямована на масштабну дезінформацію як в межах України щодо «критичної втоми від війни», міфів про «продаж» українських земель олігархам та Заходу, а також наративів про «некомпетентність» військового та політичного керівництва в умовах тотальної корупції. Так і стосовно зарубіжних партнерів, наприклад, розповсюдження тез про «неефективне використання» західної фінансової та військової допомоги, про «неминучість» перемоги росії, або ж про те, що «Україна не варта того», щоб жертвувати економічними інтересами Європи, чим руйнується єдність та довіра до України.

На наше переконання рівень протидії інформаційно-психологічній складовій російської гібридної війни вкрай низький на різних кластерах: а) нормативно-правовому (відсутність єдиної стратегії втілення проактивних (автоматизованих) заходів протидії, значні законодавчі прогалини); б) психологічному (недостатня стійкість суспільства, нерозвиненість критичного мислення); в) інституційно-комунікаційному (слабка міжвідомча координація, розпорошеність та дублювання, негнучкість державних комунікацій, відсутність єдиної дієвої платформи, яка б у режимі 24/7 об'єднувала моніторинг, аналіз та швидке формування контрнаративу, обходячи відомчі вертикалі між СБУ, ЦПД, Міністерством оборони та МЗС тощо); г) кадрово-експертному (бракує OSINT-аналітиків для превентивного виявлення ворожих наративів, фактчекерів для беззаперечного спростування фейків, а також стратегів контрпропаганди для формування сильних, емоційно резонансних і адаптованих до різних аудиторій контрнаративів); та д) технологічному (критична залежність від іноземних платформ, що проявляється в обмежених можливостях моніторингу та швидкого реагування у

кіберпросторі, обмежує суверенні спроможності України щодо глибинного аналізу та оперативного втручання для нейтралізації ворожих ІПСО).

В контексті удосконалення нормативно-правового забезпечення протидії України інформаційно-психологічній складовій російської гібридної агресії, є стратегічно доцільним адаптувати та запровадити в національне законодавство ключові принципи та зобов'язання Кодексу ЄС з практики щодо дезінформації (англ. EU Code of Practice on Disinformation [1]). Останній являє собою систему саморегуляційних стандартів, узгоджених великими гравцями цифрового ринку (онлайн-платформами, пошуковими системами, рекламною індустрією, фактчекінговими організаціями) для боротьби з дезінформацією. Серед підписантів – такі компанії, як Meta (Facebook, Instagram), Google (Search, YouTube), Microsoft (Bing, LinkedIn) та TikTok. Варто наголосити, що в 2025 році Кодекс офіційно інтегрується у рамки Регламенту (ЄС) 2022/2065 Європейського Парламенту та Ради від 19 жовтня 2022 року про єдиний ринок цифрових послуг (Digital Services Act, DSA) [2].

На переконання Тріши Меєр (доцентки кафедри цифрового управління та участі в Брюссельській школі управління Вільного університету Брюсселя, де вона очолює Дослідницький центр цифровізації, демократії та інновацій), значення цього Кодексу полягає в тому, що він є ключовим механізмом ЄС для забезпечення підзвітності дуже великих онлайн-платформ та пошукових систем (VLOPSEs) у боротьбі з онлайн-дезінформацією та системними ризиками, перетворюючись на обов'язковий Кодекс поведінки, що застосовується в рамках Закону про цифрові послуги (DSA) з липня 2025 року [3].

В межах інформаційно-психологічної складової російської гібридної війни варто згадати поширення фейкових новин російськими кібервійськами, цілеспрямоване маніпулювання громадською думкою, що набуває особливого значення під час виборчих процесів. За умов перспективного зниження інтенсивності бойових дій, виборчі процеси (президентські, парламентські та місцеві) будуть беззаперечною умовою підтримки України з боку партнерів. Звичайно, буде наявний і великий внутрішній запит на вказані виборчі процеси. Відповідно вже зараз потрібно прискіпливо вивчати досвід зарубіжних країн, де російські кібервійська провели доволі успішні виборчі кібероперації.

Для прикладу доцільно згадати недавні президентські вибори в Румунії (грудень 2024 року), де результати першого туру стали справжнім шоком та сенсацією для всього світу. Адже у першому турі переміг невідомий безпартійний ультраправий кандидат Келін Джорджеску. Як вважають багато експертів, його перемога стала результатом маніпулятивного впливу на виборців шляхом використання TikToky. Для Румунії реальною стала небезпека того, що завдяки астротурфінгу президентом виберуть прихильника теорії змови, неконструктивного критика НАТО та ЄС і шанувальника путіна.

Слід підкреслити, що астротурфінг є одним із поширених типів маніпулятивної поведінки. Це трапляється, коли якась організація штучно створює враження широкої підтримки продукту, політики чи концепції, тоді як насправді існує лише обмежена підтримка. Скоординована нещира поведінка в

Інтернеті стає дедалі серйознішою проблемою в усьому світі [4, с. 507]. При цьому зазначимо, що астротурфінг виходить за рамки онлайн-середовища. За своєю суттю, це фальшивий громадський активізм, у якому зацікавлені суб'єкти, зокрема учасники виборчих кампаній, використовують найманих осіб або ІТ-компанії для маніпулятивного створення враження народної підтримки своїх ідей, передвиборчої програми. Водночас, практика застосування астротурфінгу поширюються і на офлайн-сферу, проявляється, наприклад, у фінансуванні громадян за участь у мітингах, походах, демонстраціях, громадських слуханнях чи проплаченому збору підписів під петиціями тощо.

З огляду на наведене, перемога на полі бою або стійке припинення збройної агресії є безумовною передумовою до стійкого та безпечного повоєнного розвитку. Проте, це лише початок стратегічного шляху, оскільки ефективність відновлення та безпека повоєнної України можуть бути суттєво підірвані під впливом деструктивних російських кібернетичних та інформаційно-психологічних операцій. Усвідомлюючи цей системний ризик, готуватися до протидії невійськовим компонентам російської гібридної війни, включаючи дезінформацію та кібервплив, необхідно було вже давно, але критично важливо розпочати розбудову цих механізмів сьогодні. Саме повноцінне розуміння цих руйнівних процесів та вибудовування продуманої, довгострокової стратегії протидії невійськовим інструментам агресора є необхідною запорукою не лише успішного відновлення, але й майбутнього стійкого розвитку та процвітання Української держави.

Список використаних джерел:

1. Посилений Кодекс ЄС з практики щодо дезінформації (The Strengthened Code of Practice on Disinformation). Європейський Союз, Європейська Комісія. 16 червня 2022 р. URL: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation
2. Регламент (ЄС) 2022/2065 Європейського Парламенту та Ради від 19 жовтня 2022 року про єдиний ринок цифрових послуг та внесення змін до Директиви 2000/31/ЄС (Digital Services Act, DSA). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065
3. Trisha Meyer The EU Code of Practice on disinformation: evaluating VLOPSE compliance and effectiveness. URL: https://www.disinfo.eu/outreach/our-webinars/11-september-the-eu-code-of-practice-on-disinformation/
4. Jovi, Chan. Online Astroturfing: A Problem Beyond Disinformation. Philosophy and Social Criticism, 2024. No. 50(3), 507-528. https://doi.org/10.1177/01914537221108467