

деградація і занепад стануть неминучими супутниками майбутнього НАТО і демократичних міжнародних структур в Європі і світі.

Список використаних джерел:

1. Тодоров І.Я. Євроатлантична інтеграція України. Історія та сучасність. Навчальний посібник. Ужгород: ТОВ "Рік-У", 2022. 376 с.
2. Стратегічна концепція НАТО 2022. URL: www.nato.int/strategic-concept/#StrategicConcept

Демиденко Володимир Олексійович
професор кафедри конституційного
права навчально-наукового інституту
права та психології Національної
академії внутрішніх справ, кандидат
юридичних наук, доцент

ВІД ІМІТАЦІЇ ДО ДІЄВОСТІ: СПІЛЬНІ МУНІЦИПАЛЬНІ ЦІННОСТІ УКРАЇНИ ТА ЄС В СТРАТЕГІЇ ЗАХИСТУ ВІД АСТРОТУРФІНГУ ЯК ЕЛЕМЕНТУ СУЧАСНОЇ ГІБРИДНОЇ ВІЙНИ

Сучасна цифрова епоха радикально трансформувала поле бою, перетворивши інформаційно-комунікаційний простір на стратегічну арену. Більше того, варто наголосити, що сучасну війну можна програти ще задовго до початку відкритого військового вторгнення. Якщо програно інформаційно-комунікаційний аспект гібридної агресії, якщо зруйновано довіру, підірвано єдність та нівельовано спроможність суспільства до організованого та стійкого опору – це рівнозначно капітуляції національної стійкості на стратегічному рівні. Ескалація до збройного конфлікту в такому випадку неминуче призводить до критичної втрати державної та муніципальної керованості та стійкості.

Нині швидкість поширення інформації, анонімність мереж та доступність високотехнологічних інструментів відкрили широкі й небачені раніше можливості для зловмисників. Найбільш цинічними, підступними та цивілізаційно злочинним супротивником у цій сфері є російські кібервійська та спецслужби. На жаль, їхній стратегічний потенціал, системний характер та глобальний масштаб впливу, що ґрунтується на брехні, маніпуляціях та руйнуванні базових демократичних цінностей, часто критично недооцінюються в Україні, державах-членах ЄС та й загалом світовій спільноті. Адже мова йде про потужний, централізований державний російський кіберапарат, метою якого є не лише здійснення кібершпигунства та дезінформації, а й параліч критичної інфраструктури та демонтаж демократичних інститутів зсередини.

Ця деструктивна діяльність набуває особливої загрози на муніципальному рівні, адже атаки на місцеве самоврядування та об'єкти критичної інфраструктури громад безпосередньо підривають муніципальну безпеку та операційну спроможність демократії, паралізуючи життя громадян і поглиблюючи соціальний розкол. Їхня кінцева мета — дестабілізація

демократичних процесів та маніпуляція електоральними полями як в Україні, так і в країнах-членах Європейського Союзу, проти яких вже триває активна інформаційно-комунікаційна складова гібридної війни.

Одним із найбільш підступних та ефективних інструментів російських кібервійськ у цьому арсеналі є астротурфінг (astroturfing) – імітація "низової" громадської підтримки або протесту. Ця технологія дозволяє створювати ілюзію автентичної народної думки через мережі фейкових акаунтів, ботів та проплачених "лідерів думок", підриваючи довіру до демократичних інститутів та сіючи поляризацію в суспільствах. У контексті муніципальної влади, астротурфінг націлений на руйнування спільних муніципальних цінностей, які є фундаментом як української державності, так і європейської демократії.

У контексті муніципальної влади, астротурфінг націлений не просто на несанкціонований штучний цифровий вплив, а на цинічне руйнування самої основи муніципалізму та морального коду демократії. Адже такі спільні для демократичного співтовариства муніципальні цінності – прозорість, підзвітність, партисипативність та доброчесність є не просто муніципальними нормами чи формальними принципами муніципального управління. Вони є фундаментом соціальної консолідації та інституціональної стійкості, що критично обумовлює як життєздатність української державності в умовах зовнішньої агресії, так і цілісність європейського демократичного простору.

Варто зауважити, що нині характер російської агресії проти України зазнає стратегічної трансформації. Це пов'язано з тим, що воєнні злочинці, що входять до вищого військово-політичного керівництва московії є прихильниками концепції «гібридної війни». Як наслідок, в умовах виснаження російських ресурсів та зниження наступального потенціалу для великомасштабних конвенційних (сухопутних) операцій, агресор зміщує фокус на інші, асиметричні складові гібридної війни. Це також підтверджується аналізом бюджету російських окупантів на 2026 рік, що дає обґрунтовані підстави для гіпотетичного припущення – питома вага прямої військової агресії у загальній картині конфлікту може поступово знижуватися. Війна еволюціонуватиме 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 компонента російської гібридної війни проти України, ЄС та загалом вільного світу. Остання спрямована на масштабне інформаційно-психологічне конструювання деструктивних установок як у межах України, так і за її межами. Ці пропагандистські дезінформаційні маніпуляційні кампанії мають на меті сформувати внутрішню суспільну напругу навколо наративу «критичної втоми від війни», поширити деструктивні міфи про «розпродаж» українських земель олігархам та Заходу, нав'язати меседжі про «некомпетентність» та тотальну корумпованість військового і політичного

керівництва. Така цілеспрямована діяльність має на меті підірвати суб'єктність Української держави, зруйнувати довіру до органів влади та дезорганізувати спроможність народу до стійкого опору.

Водночас спостерігаємо нарощування російської інформаційно-психологічної компанії 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 контрнарративу, 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 контрнарративів); 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 ІІСО).

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 ТікТоку. Для Румунії реальною стала небезпека того, що завдяки астротурфіngu 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 астротурфіngu 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>

Калініченко Олександр Федосійович, професор кафедри конституційного права навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук, доцент

ІНТЕГРАЦІЯ УКРАЇНИ З НАТО В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ

Проголосивши свою незалежність і шукаючи шляхи гарантування безпеки, Україна однозначно стала на позицію входження у майбутньому в систему колективної безпеки. Сьогодні українські політики і численні пропагандистські матеріали стверджують, що вже з перших днів набуття незалежності наша держава прагнула стати членом Північноатлантичного альянсу.

Російсько-українська війна допомогла виявити найболючіші прогалини у світовій безпеці, які потребують усунення та вирішення. З іншого боку, повномасштабне вторгнення російської армії сприяло інтенсифікації взаємодії та співпраці України з державами – членами НАТО. А перший відлік цього процесу було розпочато з осені 1991 року. У Воєнній доктрині України, яка була ухвалена Верховною Радою України 19 жовтня 1993 року, у статті 1 підтверджено цей статус: “Україна виступає за створення всеохоплюючих систем універсальної та загальноєвропейської безпеки і вважає участь у них важливим компонентом своєї національної безпеки. Дотримуючись позаблокового статусу [1, с. 4].