Політологія

УДК 32:323.2

DOI https://doi.org/10.5281/zenodo.17839092

Між згодою та спротивом: адаптація теорії Джина Шарпа для протидії цифровим загрозам у Європейському Союзі

Гончар Максим Володимирович,

аспірант кафедри філософії, соціології та політології Державного торговельно-економічного університету, Київ, Україна

https://orcid.org/0000-0002-3080-5665

Прийнято: 20.11.2025 | Опубліковано: 30.11.2025

Анотація. Стаття присвячена дослідженню соціальних мереж як чинника політичної сили та вразливості Європейського Союзу в умовах гібридних загроз.Завданням статті є обґрунтування доцільності використання теорії ненасильницької боротьби Джина Шарпа, зокрема його концепції Civilian-Based Defense, для пояснення ролі соціальних мереж у забезпеченні стійкості демократичних країн ЄС. Окрім того, стаття також присвячена пошуку валідних механізмів захисту демократії, у умовах наростаючої конфронтації в цифровому просторі, зокрема в соціальних мережах, між авторитарними та демократичними системами. Фокусом роботи є адаптація практик та підходів, розроблених для класичних форм громадянського опору, у контексті безпекових викликів, породжених соціальними мережами, в Європейському союзі.

Теоретичною основою дослідження є праці Джина Шарпа (The Politics of Nonviolent Action, From Dictatorship to Democracy, Making Europe Unconquerable), в яких викладені основні принципи стійкості політичних

режимів через концепцію «стовпів підтримки» та логіку забезпечення ефективної громадянської оборони. Методологічний підхід ґрунтується на поєднанні концептуального аналізу з елементами компаративних досліджень, що дозволяє оцінити релевантність класичних концепцій ненасильницького спротиву у новому цифровому контексті.

Доведено, що підходи запропоновані Джином Шарпом ще в XX-му столітті, в умовах триваючої Холодної війни, становлять дієву аналітичну рамку, яка не втратила актуальності в сьогоденному контексті та дозволяє інтерпретувати соціальні мережі не лише як технологічний, комунікаційний чи розважальний феномен, а як простір політичний та, все частіше, військово-політичний, де вирішуються питання безпеки, впливу, згоди та легітимності влади. Адаптація концепції Civilian-Based Defense до цифрової доби відкриває можливості для розробки, чи то моделювання можливих стратегій інформаційної безпеки ЄС, в фокусі яких буде високий рівень стійкості громадян до інформаційних маніпуляцій; залучення громадянського суспільства для протидії інформаційним інвазіям; розвиток цифрової грамотності та підсилення спроможностей всього суспільства бути консолідованим, в умовах агресивної політики авторитарних режимів.

Запропонований підхід підкреслює, що сила європейських демократій може полягати не лише у площині регуляції, заборон та обмежень – спосіб, що є домінантним у більшості європейських країн нині, а й у здатності громадян цілком свідомо та зважено «відмовлятися від співпраці» з авторитарними режимами, підтримуючи та зберігаючи «цифрові стовпи» демократичного порядку.

Ключові слова: Джин Шарп, Civilian-Based Defense, Making Europe Unconquerable, соціальні мережі, цифрова стійкість, ненасильницький спротив, джерела влади, стовпи підтримки, інформаційна безпека, Європейський Союз, демократичні системи, цифрова оборона, гібридні загрози, демократична стійкість.

Between Consent and Resistance: Adapting Gene Sharp's Theory to Counter Digital Threats in the European Union

Maksym Honchar,
PhD student, Department of Philosophy, Sociology and Political Science,
State University of Trade and Economics, Kyiv, Ukraine
https://orcid.org/0000-0002-3080-5665

Abstract. The article examines social networks as a factor of political power and vulnerability of the European Union in the context of hybrid threats. The objective is to substantiate the applicability of Gene Sharp's theory of nonviolent action, particularly his concept of Civilian-Based Defense, for explaining the role of social media in ensuring Europe's democratic resilience. Furthermore, the article aims to identify effective mechanisms for protecting against the escalating confrontation in the digital space, particularly within social networks, between authoritarian and democratic systems. The focus of the study is the adaptation of practices and approaches initially developed for classical forms of civil resistance to the protection and resilience of the European Union's political system.

The theoretical basis of the research consists of Gene Sharp's works (The Politics of Nonviolent Action, From Dictatorship to Democracy, Making Europe Unconquerable), which outline six sources of power and the logic of civilian defense. The methodological framework combines conceptual analysis with elements of comparative research, enabling the assessment of the relevance of classical nonviolent resistance concepts in a new digital context.

This study elucidates approaches articulated by Gene Sharp during the twentieth century, particularly in the context of the Cold War, which constitutes an analytical framework whose relevance persists in contemporary discourse. These approaches facilitate the interpretation of social networks not solely as technological,

communicative, or entertainment platforms, but as inherently political and increasingly military-political arenas wherein issues of security, influence, consent, and the legitimacy of power are negotiated. The adaptation of the Civilian-Based Defense concept to the digital era presents significant opportunities for the formulation and modeling of European Union information security strategies. Such strategies prioritize the fortification of citizens' resilience to manipulation, the active engagement of civil society in counteracting informational incursions, the advancement of digital literacy, and the establishment of robust and sustainable communication infrastructures. This paradigm emphasizes that the resilience of European democracies is predicated not merely on regulatory or restrictive interventions – approaches that continue to predominate across much of Europe but rather on the capacity of citizens to consciously and purposefully «withdraw cooperation» from authoritarian actors, thereby sustaining and fortifying the «digital pillars» underpinning democratic order. The study's results may contribute to the development of EU policy on digital resilience and democratic safeguards.

Keywords: Gene Sharp, Civilian-Based Defense, Making Europe Unconquerable, social networks, digital resilience, nonviolent resistance, sources of power, pillars of support, information security, European Union, democratic systems, digital defense, hybrid threats, democratic resilience.

Постановка проблеми. Сучасні демократичні системи, включно з Європейським союзом, знаходяться на етапі пошуку відповідей на різноманітні виклики, спричинені частковою цифровізацією політичних процесів та нових методів ведення міжнародних протистоянь. Соціальні мережі та платформи в усьому своєму розмаїті: від особистих блогів до відеохостингів, породили ряд світоглядних та критичних питань, які безпосередньо стосуються стійкості демократичних систем. Ключові цінності та стовпи відкритих суспільств: свобода слова, приватність, право на доступ до інформації, вільні та прозорі

 ISSN: 3041-2110

вибори, можуть бути загрожениими зовнішніми акторами, метою яких є підривати та розхитувати стійкість Європейського союзу.

Цей пошук здебільшого ускладнений неоднозначністю суто регулятивних рішень та тим, що зачіпає безпосереднє питання національної безпеки як в кожній окремій країні, так і у великих наднаціональних об'єднаннях. Окрім того, проблематика породжена соціальними мережами, не може містити одноходових стратегій їх вирішення або ж «простих» рішень, оскільки перебуває в тісному переплетенні між важливістю збереження свобод та безпекових викликів водночас. Пошук «ешелонованої» захисної системи в цифровому полі ще не був запропонований в жодній з європейських країн. Методи і рішення коливаються в діапазоні від ігнорування – до жорстких заборон і обмежень. Гнучкі концепції, запропоновані класиками часів Холодної війни, можуть містити відповіді на питання: з яких частин має складатися система цифрової безпеки, що буде релевантною поточному часу та завданням, які стоять перед ЄС? В статті здійснено адаптацію теорії ненасильницького спротиву Джина Шарпа до умов цифрової політики Європейського Союзу.

Аналіз останніх досліджень і публікацій. Соціальні мережі, в сучасному контексті, перетворилися на стратегічний елемент політичної влади та безпеки. Політичні системи різного спектру, активно використовують цифрові платформи для досягнення своїх цілей, а процеси всередині мереж суттєво впливають на політичне життя, виборчі процеси, безпеку. Турбулентне середовище загострило наукові дискусії про вплив соціальних мереж на підрив демократії та демократичних інститутів по всьому світу. Ширшу рамку аналізу соціальних мереж презентує Санстейн [15], який розвиває модель публічної сфери Юргена Габермаса [8]. Він відслідковує як змінюється політична комунікація під впливом мереж. Основний напрям його досліджень стосується процесів поляризації суспільства, через формування «інформаційних коконів», що шкодить традиційним демократичним процесам.

Шошанна Зубофф у своїй роботі «The Age of Surveillance Capitalism» розглядає соціальні мереж через нову економічну логіку, яку вона називає – економіка спостереження [18]. Важливими тут стає безперервний збір, аналіз та комерція на базі даних, які вдається зібрати з користувачів і які, згодом, стають інструментом політичного процесу. В безпековому секторі, це автоматично підводить до роздумів про те, як політичні актори можуть маніпулювати цими даними, сегментуючи електорат, активно оперують алгоритмами та шкодять демократичним інститутам. Дослідник Томас Рід у праці «Active Measures», досліджує розмаїті інформаційні операції від часів Холодної війни до сучасних кампаній в цифровому полі [10]. Рід доводить, що сучасні механіки ґрунтуються на класичних підходах до дезінформації, поєднаних з інноваціями, які принесли соціальні мережі. Він говорить, що соцмережі безпосередньо стали полем для «політичної війни» («political warfare»), де хаос і атака на легітимність демократичних систем є головною ціллю авторитарних режимів.

Важливо відзначити роботу Зінгера та Брукінга «LikeWar: The Weaponization of Social Media», на думку яких, інформаційний простір є бойовищем, де перемогу одержує та сторона, яка спроможна швидше та ефективніше формувати наративи та захоплювати увагу широкої авдиторії [14]. Вони доводять, що операції в онлайн-середовищі інколи здатні перевищувати ефект від традиційних військових операцій. Схожу теоретичну рамку пропонує Девід Патрікаракос, який уводить концепт «інформаційного солдата» – користувача соцмереж, чий персональний досвід спроможний змінювати міжнародну оцінку та сприйняття конфліктів [7]. Він відзначає, що сила наративів є не менш важливою ніж сила конвенційної зброї.

Питання тактики авторитарних режимів досліджує Аліна Полякова, авторка та науковиця Центру аналізу європейської політики та Brookings Institution. Вона доводить, що операції, які провадять авторитарні режими здебільшого не мають чіткої мети в найближчій перспективі, їх завдання – підживлювати політичну фрагментацію та зберігати атмосферу хаосу [9]. Окрім

того, стратегія підриву демократичних процесів має багатовекторне спрямування: прямі дезінформаційні атаки, культивування недовіри до демократичних інститутів, вплив на міжнародну авдиторію чи спільноти діаспорян. Поглиблення розуміння соцмереж як інструменту організації протестів з їх перевагами та недоліками розглядає дослідниця Зейнеп Тюфекчі [16].

Микола Давидюк в праці «Як працює путінська пропаганда» відслідковує подібність та спадковість радянських та російських інформаційних кампаній і їх пристосування до цифрової епохи [1]. Окрім того, варто згадати авторів, роботи яких присвячені питанням національної безпеки, інформаційних маніпуляцій та гібридних загроз: Лариси Філіпенко [5], Дмитра Павленка [3], Артема Захарченка та Юлії Максімцової [17].

Таблиця 1

Підходи до цифрової безпеки в межах демократичних систем

Підхід / Автори	Основний фокус	Загрози для демократії	Методи протидії загрозам
Модель публічної сфери – Габермас [8], Санстейн [15]	Трансформація політичної комунікації	Звуження спільного простору для раціональних дебатів; зростання маніпуляцій	Регулювання платформ, прозорість алгоритмів, зміцнення медіаграмотності
Капіталізм стеження – Зубофф [18]	Економіка даних та платформ	Використання персональних даних для маніпуляцій, політичне таргетування	Контроль збору даних, обмеження корпоративного впливу, захист приватності
Політична війна та дезінформація – Рід [10], Давидюк [1]	Еволюція інформаційних операцій	Легітимна криза інститутів, зовнішні операції втручання	Інформаційна резильєнтність, державні стратегії протидії
Мілітаризація соцмереж – Сінгер і Брукінг [14], Патрікаракос [7]	Соцмережі як поле бою	Перемога через увагу, мобілізація масових емоцій	Оперативне реагування, наративна контрстратегія
Авторитарні підходи – Полякова і Мезероль [9]	Digital authoritarianism	Гібридні впливи, імпорт авторитарних тактик до демократій	Міжнародна координація, кібердипломатія
Протестні рухи та мережеві ефекти – Тюфекчі [16]	Мережевий протест, мобілізація	Нестійкість протестів, вразливість до маніпуляцій	Стійкі інфраструктури для громадянської мобілізації

Українські дослідження цифрової безпеки – Філіпенко [5], Павленко [3], Захарченко та Максімцова [17]	Національна специфіка, війна, маніпуляції	Вразливість під час війни, алгоритмічні атаки	Медіагігієна, освітні програми, інституційні протоколи

Запропонована стаття об’єднує розрізнені підходи, узагальнені в таблиці 1, в цілісну концептуальну рамку трирівневого захисту демократичних систем, яка охоплює:

1. індивідуальний рівень – медіагігієна, поведінковий опір, не-співпраця з маніпуляціями;
2. мережевий рівень – аналіз алгоритмічних динамік та інформаційних потоків;
3. інституційний рівень – політики цифрової безпеки, протидія дезінформації, розвиток резильєнтності.

Таким чином, в статті сформовані пропозиції та модель, яка демонструє, як цифрові платформи одночасно впливають на громадян, інфраструктуру мереж і політичні інститути — і як демократії можуть вибудовувати захист на всіх трьох рівнях.

Виділення невирішених раніше частин загальної проблеми. Більшість наукових досліджень в тематиці, обходить стороною питання того, в який спосіб можливо протидіяти наростаючому тиску на демократії в соцмережах. Здебільшого наголошується на важливості запровадження жорсткого контролю та значних фінансових санкціях для компаній котрі оперують та володіють різноманітними платформами та соціальними мережами. Ризики та небезпечні явища породжені соцмережами все частіше стають об’єктами наукового зацікавлення в демократичних суспільствах. Разом із тим, недостатньо осмислюються механізми, через які авторитарні режими можуть отримати відсіч та, не менш важливо, — пропорційну зворотну відповідь.

ISSN: 3041-2110

Ця стаття є доповненням і спробою розкрити можливі шляхи оформлення дієвої системи виявлення-реакції-нейтралізації атак на демократичні системи в Європі. Теоретична рамка, яку пропонує Джин Шарп зазвичай згадується у контексті революційних перетворень та ненасильницького спротиву автократіям, проте вкрай обмеженими є спроби ґрунтовних та системних досліджень, які би адаптували та описували можливості застосування дієвих та класичних формул до цифрового контексту. Спадщина Джина Шарпа є однією з таких моделей, яка зокрема є важливою в трикутнику громадяни – влада – стороні актори, де громадяни є суб'єктом і важливим елементом протидії. Саме тому, в статті буде приділену увагу механізму «не співпраці» з кампаніями та організованими атаками на демократичні суспільства.

Формулювання цілей статті

- Метою цієї статті є інтеграція теоретичної спадщини Джина Шарпа у дослідження ролі соціальних мереж у зміцненні та захисті Європейського союзу перед обличчям інформаційних та гібридних загроз; дослідження має прикладну спрямованість у сфері політичної безпеки;
- Розрити, в який спосіб концепція громадянської оборони, адаптована до умов цифрової доби, може стати один з елементів європейської стратегії «цифрової нездоланності» – стану, коли соціальні мережі сприяють стійкості демократичних держав Європи.
- Розглянути можливі стратегії протидії авторитарним режимам в цифровому середовищі та соціальних мережах та сформулювати принцип «цифрової громадянської безпеки».

Виклад основного матеріалу дослідження. У XX-му столітті стратегічну стабільність поствоєнного європейського континенту формували військові союзи, баланс ядерних сил і система колективної оборони, підкріплена економічними вигодами та митними спрощеннями. У XXI-му столітті ці чинники доповнились новим, вкрай уразливим, виміром – цифровим. Соціальні мережі, що спочатку сприймались як інструмент глобальної

комунікації та демократизації інформаційного простору, стали водночас і інструментом війни, і безпосереднім полем боротьби, і безпековим елементом. Їхня подвійна природа – можливість одночасно зміцнювати та підривати демократичні інститути є важливим фактором політичної стійкості кожної європейської країни, та ЄС в цілому.

Соціальні мережі та платформи зростали та набирали ваги паралельно із трансформаціями, кризами та конфліктами, протягом останніх десятиліть. Їх вплив та роль почала осмислюватися науковцями у нестабільному геополітичному контексті, котрий означений подіями на кшталт «арабської весни» чи російської агресії проти України. Гібридні загрози, зокрема інформаційні операції, цілеспрямовані кібератаки, маніпуляція алгоритмами та використання сіток ботів, перетворили соціальні медіа на поле, де геополітичне суперництво відбувається в режимі реального часу.

Проблематика, з якою нині стикається ЄС, полягає у відсутності цілісної теоретичної моделі та напрацьованої візії, що дозволяла б розглядати соціальні мережі, не як загрозу, а радше інструмент стримування та протидії агресивній політиці режимів з-за меж Європейського союзу. Соціальні мережі та платформи, стали свого роду «заручниками» у широкому протистоянні радикально різних систем та світоглядів. Їх глобалістична природа та глибока проникність у суспільства витворила незвичний тип конфлікту який, все ж, пролягає між авторитарними та демократичними системами. Зі схожою проблематикою світ стикався в часи Холодної війни, яку нерідко припасовують задля пояснення подій сучасних. В цьому ключі доречно було б запропонувати гіпотезу: чи можна використати напрацювання, ідеї та стратегії, створені в минулому столітті для протидії агресії та авторитарному тиску нині – у цифровому середовищі?

Для опрацювання цієї гіпотези, звернемося до праць Джина Шарпа – одного з ключових дослідників ненасильницького спротиву та автора класичних праць, які доводять, що демократичні суспільства можуть ставати

 ISSN: 3041-2110

«нездоланними» навіть без застосування чи опертя на збройної сили, якщо вони володіють відповідними навичками організованого, скоординованого і морально обумовленого легітимного опору. У своїх працях «Від диктури до демократії»[6], Making Europe Unconquerable (1985) [12] та Civilian-Based Defense (1990) [11] він описує надважливу концепцію «громадянської оборони» – системи, у якій кожен громадянин є суб'єктом та важливим учасником процесу відсічі потенційній агресії. Шарп спирається на ідею того, що влада агресора завжди обмежена ресурсами, вона оперта на «співпрацюючих» з режимом і має підпорядковане собі суспільство. Разом із тим, він доводить, що у випадку, коли ці складові поступово чи цілковито руйнуються – втрачається і потенціал до агресії, а згодом і сама влада.

Безпекова сфера та тканина влади, таким чином, доповнюється додатковим виміром. Якщо XX-те століття було епохою де питання національної безпеки «замикалася» на питаннях прихильності тій чи іншій ідеології, територій, кордонів, сталості державних інституцій, великих військово-політичних альянсів, то у XXI-му столітті система національної безпеки ускладнилася, отримавши новий сектор – цифрове середовище. Окрім розгалуження потоку інформації, яку щодня отримують громадяни того, чи іншого суспільства, пропорційною стала роль баталій за колективну пам'ять та здатність суспільства зберігати спільну інтерпретацію реальності, цілісність якої досить складно втримувати в умовах швидкого вдосконалення «діпфейків», софістикованої дезінформації та маніпулятивних повідомлень в соціальних мережах чи інтернеті.

Традиційна, дещо патримоніальна, схема відповіді на цей виклик передбачає жорстку реакцію держави, яка відповідає за інформаційну безпеку громадян. Водночас, ця формула є неактуальною, адже за своїм смислом походить з, того ж таки, XX-го століття, в якому заборонна та фільтрація «небажаної» інформації була способом відповідати на взаємну дискредитацію між блоками, що знаходилися по два боки «Залізної завіси». Досвід минулого,

докладно описаний Пітером Померанцевим у новій роботі «Як виграти інформаційну війну?», доводить, що комунікаційні важелі впливу на опонента можуть бути вкрай дієвими, коли вони виконують не лише інформаційну роль, але і активно протидіють у відповідь [4]. Радіо – своєрідний символ минулого століття, застосовувалося з подвійною функцією: воно було засобом підтримання легітимності та, водночас, інструментом війни. Схожа логіка проглядається і в соціальних мережах які можуть бути або інструментом захисту, або джерелом руйнації – залежно від того, наскільки ефективно суспільство пристосоване до того, щоб організовувати ненасильницький спротив у цифровому просторі.

Теоретичний підхід Джина Шарпа слугує певним «каркасом», який дозволяє розглядати громадян, як актора, котрий підсилює спроможності демократичної системи до протидії. Шарп спирається на внутрішню мобілізацію суспільства, без залучення зовнішньої допомоги і цей принцип є важливим, адже він не вимагає включеності чи втручання третіх сторін, що у випадку ЄС, відкриває простір національним уряд діяти без очікування та консультацій про рішення у форматі всього європейського об’єднання, де демократичний процес вироблення нових політик є тривалим та складним. Окрім того, Шарп приділяє увагу питанню збереження довіри всередині спільнот, яка є фундаментом стійкої демократії, та тією точкою, де авторитарії прагнуть найбільше здійснювати свій вплив та тиснути, роздмухуючи суперечності і атомізуючи населення демократичних країн.

Основна ідея Джина Шарпа напрочуд проста, але водночас спостережлива: політична влада не є абсолютом, який політики міцно тримають у своїх руках – це своєрідна співзалежність між політичним лідером чи автократом, що підтримується згодою та співпрацею підкорених і керованих. Міцність будь-якого режиму та влади, в такому випадку, може слабшати не лише від прямого насильницького тиску, а й від організованого припинення співпраці. У своїй праці «The Politics of Nonviolent Action» Шарп послідовно

розкладає ті джерела, через які влада «постачається»: авторитет, людський капітал, навички та знання, нематеріальні чинники (віра, звичаї, наративи), матеріальні ресурси. Ідею про підживлення влади від цієї співпраці він розвиває і в роботі From Dictatorship to Democracy у розділі «Whence Comes the Power?», де наголошено, що будь-який режим — навіть найжорсткіший — функціонує лише доти, доки люди, інституції та групи забезпечують йому необхідні ресурси [13].

Звідси ми маємо наступний теоретичний рівень. Допускаючи, що джерела влади є глибоко залежними від її «постачальників», то владу можливо обмежити або зруйнувати без втрати людського капіталу чи матеріальних збитків, достатньо лише «відключити» політичного актора від «джерела живлення» – організовано відмовитися постачати ресурси для його існування. Саме цей підхід названий «ненасильницькою боротьбою», що, разом із тим, не передбачає пасивну опозицію чи моральне несхвалення, а є відпрацьованою та злагодженою стратегією з демонтажу системи.

Автор також уводить поняття «стовпи підтримки» (pillars of support). За ним, будь-який політичний режим тримається на низці інституцій, груп і практик, котрі раз у раз підживлюють його спроможність ухвалювати та впроваджувати управлінські рішення: від профспілок, поліції, армії, розгалуженої бюрократії, до медіа, судів і церковних структур. А у сучасному контексті, ще і від цифрового середовища. У випадку, коли ці «стовпи» обмежують або припиняють співпрацю – через страйки, саботаж, публічні заяви, моральний осуд, економічний тиск, режим втрачає важелі керування та переходить у стан кризи [6].

Ця ідея є універсальною і дозволяє однаково пояснювати як динаміку авторитарних, так і демократичних систем. Важливо, що в реаліях Європейського Союзу, де демократична легітимність спирається на стійкість інституцій та довіру громадян, цей механізм стає однією з основних цілей зовнішніх атак. Авторитарні режими проактивно працюють на підрив цих

 ISSN: 3041-2110

«стовпів» – наприклад, атакуючи довіру до виборчої системи, медіа чи міжнародних структур ЄС. Показовим є приклад кампаній дезінформації під час референдуму щодо Brexit, де соціальні мережі стали каналом для таргетованих меседжів, спрямованих на ключові сегменти електорату. Хоча ця подія відбувалася у межах однієї держави, її наслідки вплинули на геополітичну архітектуру всієї Європи.

Перенесення цієї концепції в цифрове середовище не є простою «технологічною адаптацією». Соціальні мережі змінили саму природу простору, де відбувається взаємодія між владою, громадянами та потенційним агресором. Інформаційні атаки, кампанії з дезінформації, підрив довіри до інституцій – усе це може відбуватися без фізичної присутності супротивника чи опонента. У цифровій логіці агресор не має потреби окупувати територію – йому достатньо окупувати інформаційні канали та когнітивний простір цільової аудиторії.

Аналіз подій останніх років демонструє, що авторитарні держави, насамперед Росія та Китай, цілеспрямовано використовують соціальні мережі для підриву ключових елементів європейських демократій – від довіри до виборчих інститутів до легітимності наднаціональних структур ЄС [9]. Кампанії дезінформації під час президентських виборів у Франції 2017 року, виборів до Європарламенту 2019 року, а також постійні інформаційні операції щодо теми міграції чи енергетичної безпеки ілюструють здатність супротивника адаптувати меседжі під локальний контекст і використовувати лінії розламів та напруженості всередині держав.

З точки зору Шарпа, це можна описати як «повільне руйнування» елементів легітимності влади. Тут замість прямого конфлікту, відбувається розмивання довіри та посилення поляризації, що врешті знижує здатність суспільства до консолідованого спротиву – внутрішні суперечності, «підігріті» третьою силою розмивають ризик та значення загрози з-боку авторитарних систем. Ключовим є те, що такі атаки часто непомітні на початковому етапі,

 ISSN: 3041-2110

адже вони працюють через локальних акторів і «здаються» органічними для внутрішнього інформаційного поля.

Це має дві ключові наслідки та точки вдосконалення для безпекових політик в ЄС. По-перше, громадянська оборона не має бути лише сценарієм «на випадок війни», натомість має перетворюватися на постійну систему протидії гібридним загрозам. По-друге, акцент зміщується з мобілізації населення у кризовий момент на довгострокове формування культури інформаційної стійкості. У «Making Europe Unconquerable» Шарп наголошує, що такий вид оборони вимагає «попередньо підготовлених структур» – у цифровому контексті це означає створення мережевих спільнот, здатних автономно виявляти і нейтралізувати маніпулятивні наративи [12].

Показовим прикладом такого підходу є досвід Литви, Латвії та Естонії, які після масованих кібератак та дезінформаційних кампаній з боку Росії у 2007–2014 роках розбудували цілісну систему цифрової оборони, де важливу роль відіграють не лише державні кіберпідрозділи, але й волонтерські мережі фактчекерів, журналістів та активістів. Це, свого роду, цифрова форма ненасильницького опору, яка не вимагає включеності державної влади та безпекових інституцій. Подібні підходи впроваджуються і в Скандинавії: Швеція, з огляду на багаторічний досвід протидії радянській пропаганді, інтегрувала медіаграмотність та аналіз джерел інформації у шкільну програму, створивши «превентивний щит» ще на рівні освіти. Це втілення однієї з ключових тез Шарпа, згадної раніше, що «здатність до спротиву має виховуватися задовго до моменту атаки» [12].

Таким чином, цифрова громадянська оборона перестає бути пасивним інструментом реагування і перетворюється на активну політику стримування. Для Європейського Союзу це означає необхідність стратегічного усвідомлення, що інформаційний простір є не менш важливим полем боротьби за безпеку, ніж традиційні військові та економічні сфери. Перегорнувши логіку Шарпа, доходимо висновку: якщо влада тримається на згоді керованих – у цифрову

добу це означає, що втрата довіри громадян в цифровому просторі через алгоритми та механізми соцмережах може стати тим самим «мирним переворотом», тільки не зсередини, а під впливом зовнішніх сил.

Ще один важливий момент в шарпівській теорії – це, так зване, «політичне джиу-джитсу», або ж зворотна хвиля від репресій та утисків, застосованих проти групи, яка чинить ненасильницький спротив. Тут домінує логіка, за якою, несправедливі репресії та застосування сили спрацьовують проти режиму: вони руйнують джерела її влади – легітимність, моральну перевагу, звичку до підпорядкування – і, нерідко, мобілізують спостерігачів, які були пасивними до того. Саме тому, тотальний контроль чи суттєві обмеження в мережах, можуть викликати в громадськості зворотну реакцію – невдоволення і спрацьовувати проти урядів, що намагаються стримати безконтрольне поширення інформації.

На перший погляд, видається, що ці напрацювання підходять лише для аналізу «офлайн» сценаріїв або інших політичних процесів, шо відбуваються «наживо» і стосуються змін політичних режимів, революцій, повстань та кольорових революцій. Однак, сам Шарп не обмежується конкретним технологічним укладом, він лише пояснює як працює логіка та архітектура «співпраці» між політичним режимом і громадянами. Він надає ширшу картинку того, як механізми ненасильницької протидії можна застосувати в соціальних мережах. Шарп у «Making Europe Unconquerable» також ставить питання про те, як зробити європейські країни «нездоланними», виключаючи з теорію військову силу [12]. Він стверджує, що організована не-співпраця з агресором, збереження паралельних каналів комунікації та управління, моральна мобілізованість громадян та міжнародна солідарність – стають ефективними важелями опору у ситуації, коли потрібно протистояти відкритій агресії.

В який спосіб застосувати ці підходи у добу платформ і алгоритмів? Тут потрібно окремо зазначити, що соціальні мережі не просто «медіа» чи

комунікаційні майданчики, а один із тих самих «стовпів підтримки», які описує Шарп в роботі «The Politics of Nonviolent Action». Авторитет у цифрі набуває форми репутації, позначеної маркерами верифікації й алгоритмічними рейтингами; людський капітал – це мережі підписників, модераторів, волонтерів, інституцій; знання і навички – це цифрова грамотність, методи верифікації, OSINT-практики, спроможність працювати зі складністю наростаючого інформаційного потоку; нематеріальні чинники – це наративи, меми, символи; матеріальні ресурси – платформи, дата-центри, платіжні системи, тощо. Санкції – це політики модерації, заборони, а також правові приписи. У цьому сенсі соціальні мережі – це «магістралі», які так само постачають владу, а отже вони працюють за принципами схожими до «аналогових» [13].

Системність теорії Джина Шарпа дозволяє побачити важливу трирівневу структуру захисту. Перший аспект розгортається на рівні індивідів – як культивація навичок не-співпраці з маніпуляцією: медіагігієна, мінімізація участі у ланцюгах поширення токсичного контенту, тощо. Більше того, індивідуальна здатність виявляти та свідомо відмовлятися від «співпраці» з шкідливими наративами в соціальних мережах є наріжним каменем ефективної нейтралізації потенційних атак. Якщо зусилля, витрачені на підрив демократії в ЄС, не знаходять відгуку – втрачається сенс їх подальшого масштабування. На наступному рівні спільнот – йдеться про побудову альтернативних каналів, які не залежать від примхи одного приватного медіуму, це в, свою чергу, вимагає розбудови етичних кодексів, що утримують суспільство в балансі, відмовляють у мові ворожнечі між учасники спільноти та створюють спільні правила «співжиття» в просторі соціальних мереж та платформ. На третьому рівні інституцій і держав – як планування «цифрової громадянської оборони» у мирний час. «Цифрова» громадянська оборона цілком адаптується до підходів, які запропоновані для громадянської оборони офлайн-формату: підготовка кадрів, симуляції криз, правові рамки прозорості алгоритмів, узгоджені

 ISSN: 3041-2110

протоколи між платформами і громадськими структурами на випадок кризового відключення або масованої дезінформації. Така інфраструктура, з акцентом на роль кожного у свідомій відмові співпрацювати з руйнівними впливами, дозволяє децентралізувати відповідальність за інформаційну безпеку в соцмережах. Для цифрової доби це означає відхід від виключно реактивної модерації і боротьби з «окремими фейками» до формування структур, які зменшують саму можливість експлуатації «стовпів підтримки» авторитарними акторами.

Шарп протиставляє одноразові кампанії – реакції лише постфактум – культурі прогнозування і превентивного розгортання громадянської оборони. Вона розглядається не як пасивна оборонна конструкція, а як динамічна система, що здатна діяти на випередження, зберігаючи моральний стійкість та суверенітет навіть у разі тривалої зовнішньої загрози [12]. Перенесення цієї логіки у цифровий простір Європейського Союзу вимагає глибокого переосмислення: йдеться не лише про створення захисних механізмів, а про визнання факту, що цифровий простір ЄС вже є театром систематичних атак з боку авторитарних держав, а отже вимагає складнішої системи їх нейтралізації .

Важливим наслідком такої постановки питання є переорієнтація з суто оборонної моделі на проактивну стратегію. Це передбачає не лише нейтралізацію шкідливих впливів, але й цілеспрямоване формування стійкої цифрової культури. Якщо авторитарні режими намагаються розхитати підтримку демократичних інституцій, то стратегія ЄС має будуватися на їх активному зміцненні. Разом із тим, лишається нерозритою відповідь на питання чи мають демократичні системи лише захищати свій простір чи мають легітимне право здійснювати активні акції-відповіді? На це питання ще в 2008-му році відповідав Едвард Лукас у своїй роботі «Нова Холодна війна», де було проілюстровано, що вічна оборона – це прямий шлях до програшу в протистоянні [2]. Він доводить, що «гасіння пожеж» призводить до відставання,

натомість він пропонує логіку «контрнаступу» в інформаційному полі. Вочевидь, цей четвертий рівень ще має закріпитися в європейських стратегіях, котрі, навіть попри широкомасштабну агресію РФ про України, лишаються досить стриманими і не передбачають активного руйнування «стовпів підтримки» в державах-опонентах.

Таким чином, використання Шарпівської концепції дозволяє розглядати цифрову громадянську оборону ЄС не як вузьку технологічну проблему, а як багаторівневу соціально-політичну систему, у якій оборона, контрнаступ і моральне лідерство взаємопов'язані. Європейський Союз, визнаючи, що він вже перебуває під прицілом авторитарних інформаційних операцій, має переосмислити свою роль у цьому конфлікті: від об'єкта захисту – до суб'єкта, здатного формувати власний порядок денний у цифровому просторі та соціальних мережах [11,12].

Не менш важливими є подальші розробки цілісної моделі громадянської оборони для українського контексту. Як було продемонстровано вище, впливи авторитарних систем в полі соціальних мереж і платформ становлять значну загрозу для стійкості демократичних систем. Перебуваючи у тривалій війні, Україна змушена протистояти безпрецендентним атакам на своє мідаполе, котре безумовно включає і його цифровий вияв. В цій ситуації напрацювання в українських громадян спроможності «не співпраці» з агресивним авторитарним режимом – є одним із найважливіших елементів національної безпеки, адже соціальні мережі стають простором, де РФ здійснює вербування з метою подальшого деструктивного впливу на оборону та створення хаосу в тилу української демократії.

Висновки. Аналіз теорії Джина Шарпа в контексті впливу соціальних мереж на політичну стабільність Європейського Союзу показує, що його концепції залишаються не лише історично релевантними, але й напрочуд адаптивними до нової цифрової реальності. Підхід Шарпа до влади як до системи «стовпів підтримки» дозволяє ідентифікувати критичні точки, через які

авторитарні режими здійснюють інформаційний тиск. Перенесення цього аналітичного інструментарію в площину сучасних медіа дозволяє не просто описати механізми впливу, а й вибудувати ефективну модель їхнього упередження.

З огляду на досвід інформаційних кампаній проти окремих держав ЄС, стає очевидно, що соціальні мережі – це не лише платформа для громадянської мобілізації, але й поле гібридної конфронтації, де авторитарні актори свідомо атакують найбільш вразливі «стовпи підтримки» демократичних систем: довіру до інститутів, єдність політичної спільноти, незалежність медіа. Підхід Шарпа дозволяє не просто фіксувати ці атаки постфактум, а й конструювати запобіжні механізми.

Особливу вагу в цьому контексті набуває концепція Civilian-Based Defense, докладно викладена в Making Europe Unconquerable. Для ЄС вона пропонує парадигму, у якій стійкість до цифрових загроз досягається не лише технологічними інструментами (модерацією контенту, кібербезпекою), але й довгостроковим формуванням громадянської готовності – культури критичної взаємодії з контентом в соцмережах, міжінституційної координації та громадянського суспільства

Європейський Союз, стикаючись із системними інформаційними атаками, не може обмежуватися виключно реактивними діями. Відповідно до напрацювань Джина Шарпа ефективна стратегія безпеки має бути проактивною, передбачати можливі вектори впливу, системно зміцнювати ключові «стовпи підтримки» та створювати умови, за яких авторитарні наративи втрачають силу ще до того, як потраплять у широкий інформаційний обіг. Таким чином, впровадження принципів ненасильницького спротиву в інформаційний простір та розгортання багаторівневої системи «цифрової громадянської оборони» стає не лише етичним, а й стратегічним імперативом для збереження політичної суб'єктності та єдності Європи. Підсумовуючи, варто відзначити, що подальші розробки запропонованої моделі та адаптація

 ISSN: 3041-2110

класичних праць часів Холодної війни, може бути базою для підготовки для розроблення освітніх і комунікаційних програм цифрової громадянської стійкості, спрямованих на підвищення критичного мислення, медіаграмотності та здатності суспільства протидіяти маніпулятивним практикам у мережевому середовищі.

Список використаних джерел

1. Давидюк, М. *Як працює путінська пропаганда* [in Ukrainian]. Київ: Vivat, 2018. 256 с.

2. Лукас, Е. *Нова холодна війна. Як Кремль загрожує і Росії, і Заходу* [Електронний ресурс] [in Ukrainian]. Київ: Темпора, 2009. 486 с. Режим доступу: https://irbis-nbuv.gov.ua/cgi-bin/ua/elib.exe?Z21ID=&I21DBN=UKRLIB&P21DBN=UKRLIB&S21STN=1&S21REF=10&S21FMT=online_book&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=FF=&S21STR=ukr0001879 (дата звернення: 02.09.2025).

3. Павленко, Д. Динаміка сучасних соціальних медіа в Україні в контексті підтримки інформаційної безпеки [Електронний ресурс] [in Ukrainian] // *Наукові праці Національної бібліотеки України імені В. І. Вернадського*. 2023. Вип. 67. С. 108–117. Режим доступу: https://nbuviap.gov.ua/images/e_biblioteka/naukovi_resursi/Socialni%20komunikacii/Pavlenko%20D.%20Dinamika%20sucasnih%20socialnih%20media.pdf

4. Померанцев, П. *Як виграти інформаційну війну. Пропагандист, який перехитрив Гітлера* [in Ukrainian]. Чернівці: Meridian Czernowitz, 2025. 400 с.

5. Філіпенко, Л. В. Роль соціальних мереж у формуванні суспільної думки під час російсько-української війни [Електронний ресурс] [in Ukrainian] // *Соціополіс: журнал соціальних та політичних наук*. 2024. № 1. С. 10–19. Режим доступу: https://www.sociopolis.in.ua (дата звернення: 17.08.2025).

6. Шарп, Д. *Від диктатури до демократії: концептуальні засади визволення* [Електронний ресурс] [in Ukrainian]. Boston: The Albert Einstein Institution, 1993. Режим доступу: https://www.nonviolent-conflict.org/resource/from-dictatorship-to-democracy-a-conceptual-framework-for-liberation-ukrainian/ (дата звернення: 02.08.2025).

7. Patrikarakos, D. *War in 140 Characters: How Social Media Is Reshaping Conflict in the Twenty-First Century*. New York: Basic Books, 2017. 320 p.

8. Habermas, J. *The Structural Transformation of the Public Sphere*. Cambridge: MIT Press, 1989. 301 p.

9. Polyakova, A., & Meserole, C. *Exporting Digital Authoritarianism: The Russian and Chinese Models* [Електронний ресурс]. Brookings Institution, Democracy & Disorder Policy Brief, 2019. 22 p. URL: https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf (date of access: 29.08.2025).

10. Rid, T. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux, 2020. 528 p.

11. Sharp, G. *Civilian-Based Defense: A Post-Military Weapons System*. Princeton, NJ: Princeton University Press, 1990. 165 p.

12. Sharp, G. *Making Europe Unconquerable: The Potential of Civilian-based Deterrence and Defense*. Cambridge, MA: Ballinger Publishing Company, 1985. 213 p.

13. Sharp, G. *The Politics of Nonviolent Action*. Boston: Porter Sargent, 1973. 893 p.

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

15. Sunstein, C. R. *#Republic: Divided Democracy in the Age of Social Media*. Princeton: Princeton University Press, 2017. 310 p.

16. Tufekci, Z. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. New Haven: Yale University Press, 2017. 360 p.

17. Zakharchenko, A., Maksimtsova, Yu., Iurchenko, V., Shevchenko, V., & Fedushko, S. *Under the Conditions of Non-Agenda Ownership: Social Media Users in the 2019 Ukrainian Presidential Elections Campaign* [Електронний ресурс]. arXiv preprint, 2019. 21 p. Режим доступу: https://arxiv.org/abs/1909.01681 (дата звернення: 07.09.2025).

18. Zuboff, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019. 691 p.

 ISSN: 3041-2110